ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

CARRERA: INGENIERÍA EN CONTABILIDAD Y AUDITORÍA C.P.A.

TRABAJO DE TITULACIÓN

TIPO: Proyecto de Investigación

Previo a la obtención del Título de:

INGENIERA EN CONTABILIDAD Y AUDITORÍA C.P.A.

TEMA:

AUDITORÍA INFORMÁTICA A LA UNIDAD DE GESTIÓN TECNOLÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO, PROVINCIA DE TUNGURAHUA, PERÍODO 2016.

AUTORA:

JOHANNA DEL CARMEN VILLENA GÓMEZ

RIOBAMBA – ECUADOR

2019

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de titulación, ha sido desarrollado por la Srta. Johanna del Carmen Villena Gómez, quien ha cumplido con las normas de investigación científica y una vez analizado su contenido, se autoriza su presentación.

Ing. Willian Geovanny Yanza Chávez	Dr. Carlos Volter Buenaño Pesántez
DIRECTOR DEL TRIBUNAL	**MIEMBRO DEL TRIBUNAL**

DECLARACIÓN DE AUTENTICIDAD

Yo, Johanna del Carmen Villena Gómez, declaro que el presente trabajo de titulación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación.

Riobamba, 10 de enero de 2019

_____

Johanna del Carmen Villena Gómez
C.C.: 180435742-2

DEDICATORIA

Este *trabajo de investigación, cuando apenas comenzó como una idea que poco a poco y con un gran esfuerzo se llegó a concretar, lo dedico principalmente a Dios, por dotarme de sabiduría y paciencia para alcanzar esta meta más en mi vida.*

A mis papis Manuel y Mercedes, por apoyarme en cada decisión y cada paso hasta llegar donde hoy me encuentro.

A mis familiares y amigas quienes con una u otra palabra de aliento me apoyaron, en especial a Sor Ana María Beltrán, conjuntamente con sus oraciones me acompaño en este camino.

Johanna Villena Gómez (Joy)

AGRADECIMIENTO

Al *culminar el presente trabajo de investigación quiero agradecer*

A la Escuela Superior Politécnica de Chimborazo y docentes por formar profesionales capaces de desenvolverse en el medio actual.

A mis padres por apoyarme e inculcarme valores que han contribuido a mi desarrollo personal.

Al Doctor Manuel Caizabanda, Alcalde del GAD Municipal del Cantón San Pedro de Pelileo, así como a los funcionarios del mismo, Ingeniero Luis Carrasco, Ingeniero Julio Flores, Ingeniero Miguel Guato, también a una persona única, quién me apoyo incondicionalmente, Doctora Yajaira Villarroel, agradezco la oportunidad y colaboración para la realización del presente trabajo.

También quiero agradecer a mis mentores, Ingeniero Willian Yanza y Doctor Carlos Buenaño, quienes con paciencia, así como, su experiencia y conocimientos, me guiaron durante el desarrollo del presente trabajo.

Johanna Villena Gómez (Joy)

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

En el presente trabajo de investigación, se llevó a cabo la Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016; con el fin de evaluar la seguridad de la información. Con respecto a la metodología se aplicó el Marco Integrado de Control Interno COSO I; de acuerdo a lo que establece la Contraloría General del Estado, que sirvió como base para la elaboración de los cuestionarios; que permitieron identificar los hallazgos que inciden en la integridad, confiabilidad y confidencialidad de la información. Además, se elaboraron indicadores de eficiencia de los recursos; eficacia en los procesos de la Unidad de Gestión Tecnológica, también indicadores presupuestarios; que evidencian la participación presupuestaria de la unidad mencionada con respecto al presupuesto institucional. Por tanto, se identificaron hallazgos como falta de cámaras de seguridad, plan estratégico informático desactualizado e inexistencia de normativa con respecto al diseño e instalación del Centro de Procesamiento de Datos. Finalmente, al concluir las fases de la Auditoría Informática se emitió el Informe en el cual se recomienda al Señor Alcalde, Concejo Municipal y personal encargado del manejo de la información; elaborar y ejecutar proyectos que contribuyan a salvaguardar los activos informáticos y garantizar la integridad, confiabilidad y confidencialidad de la información de la institución.

Palabras claves: <CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS> <AUDITORÍA INFORMÁTICA> <TECNOLOGÍA DE LA INFORMACIÓN> <CONTROL INTERNO> <INDICADORES> <PELILEO (CANTÓN)>

Ing. Willian Geovanny Yanza Chávez

DIRECTOR DEL TRABAJO DE TITULACIÓN

SUMMARY

In this research work, the Informatics Audit was carried out to the Technological Management Unit of the Gobierno Autonomo Descentralizado Municipal of the Canton San Pedro of Pelileo, Province of Tungurahua, period 2016, in order to evaluate the security of the information. According to the methodology COSO (Committee of Sponsoring Organization of the Treadway Commission I) was applied, according to Contraloria General of the Estado. It served as the basis for the elaboration of the questionnaires; that identified the findings that had an impact on the integrity, reliability and confidentiality of information. In addition, indicators of resource efficiency, efficiency in the processes of the Technological Management unit, budgetary indicators that show the budgetary participation of the unit with respect to the institutional budget were elaborated. Therefore, findings were identified such as the lack of security cameras, an outdated computer strategic plan and the absence of regulations regarding the design and installation of the Data Processing Center. Finally, at the conclusion of the phases of the Informatics Audit, the report recommends to the Mayor, Municipal Council and personnel in charge of information management, to elaborate and execute projects to contribute the safeguard of the computer assets and guarantee the integrity, reliability and confidentiality of the information of the institution.

Keywords: <ECONOMIC AND ADMINISTRATIVE SCIENCES>, <INFORMATIC AUDIT>, <INFORMATION TECHNOLOGY>, <INTERNAL CONTROL>, <INDICATORS>, <PELILEO (CANTON)>

INTRODUCCIÓN

En la actualidad el uso de las Tecnologías de la Información y Comunicación forma parte de la vida cotidiana, llevándola al punto de convertirse en la denominada Era Digital, y a la vez generando efectos positivos y a la vez negativos. Ante esto, las instituciones tanto públicas como privadas deben precautelar la seguridad de la información, considerada como un activo muy valioso, por lo que mantener la integridad, confidencialidad y disponibilidad de la misma es una prioridad, así como la protección y mantenimiento de los equipos informáticos para el desarrollo de las actividades laborales.

El presente trabajo de investigación denominado como Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, tiene como objetivo evaluar la seguridad de la información y su desarrollo se detalla a continuación:

CAPÍTULO I: Contiene el planteamiento, formulación y delimitación del problemas, así como la justificación y objetivos del presente trabajo de investigación.

CAPÍTULO II: Corresponde a los antecedentes investigativos que fueron considerados una guía para la realización del presente trabajo de investigación, además se aprecia el Marco Teórico en donde se citan autores con respecto a las variables como son la Auditoría y la Seguridad de la Información.

CAPÍTUO III: Se refiere al Marco Metodológico, el tipo de investigación, los métodos, técnicas e instrumentos utilizados para el desarrollo del presente trabajo de investigación.

CAPÍTULO IV: Denominado Marco Propositivo, que atañe al desarrollo de la Auditoría Informática en sus tres fases: Planificación, Ejecución y Comunicación de Resultados para obtener el producto final que es el Informe de Auditoría Informática.

CAPÍTULO I: EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Pelileo es uno de los nueve cantones de la Provincia de Tungurahua, creado mediante decreto expedido por el Gobierno Provisorio el 3 de Julio de 1860, fundado como tal el 22 de julio, e inició su vida municipal el 31 de julio del mismo año; la municipalidad se acopla a lo que establece la Constitución de la República del Ecuador sobre la autonomía política, administrativa y financiera de los gobiernos autonómos descentralizados conjuntamente con los principios de solidaridad, subsidariedad, equidad, interterritorialidad, integración y participación de los ciudadano (Art. 238). En concordancia con el Código Orgánico de Organización Territorial, Autonomía y Descentralización – COOTAD – sobre la personería jurídica, derecho público y autonomía de los gobiernos autónomos descentralizados municipales; además establece que la sede del gobierno autónomo descentralizado municipal será la cabecera cantonal prevista en la ley de creación del cantón. (Art. 53)

Mediante observación directa y diálogo con el personal del área a ser auditada, las debilidades encontradas se detallan a continuación: el centro de procesamiento de datos y los equipos informáticos no cuentan con una póliza de seguros que los cubra en casos fortuitos, lo que provocaría una pérdida total o parcial de los equipos y de la información de la Institución; las instalaciones físicas no son adecuadas, siendo vulnerable ante diversas situaciones como: cambios de temperatura, incendios, goteras en las instalaciones, ceniza volcánica exponiendo a peligros al personal que labora en la unidad mencionada y unidades administrativas aledañas; la unidad objeto de estudio no dispone de cámaras de seguridad, ni controles de acceso al mismo. Finalmente no cuentan con indicadores sobre el nivel de eficiencia en cuanto al uso de los equipos informáticos, incidiendo en la optimización de los mismos.

De acuerdo a las debilidades identificadas es importante realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

1.1.1. Formulación del Problema

¿Cómo la Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, mejorará la seguridad de la información de la institución?

1.1.2. Delimitación del problema

Campo de Acción: Auditoría

Objeto de Estudio: Auditoría Informática

Espacio: Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo

Tiempo: Período 2016

Aspecto: Cumplimiento de la Norma 410 establecida por la Contraloría General del Estado

1.2. JUSTIFICACIÓN

El desarrollo del presente trabajo de investigación se justifica desde la perspectiva teórica mediante la consulta bibliográfica y linkográfica que fundamenta la base científica del marco teórico sobre definiciones de varios autores en cuanto a: clasificación de la auditoría, control interno basado en el COSO I, fases de la auditoría, riesgos de auditoría y riesgos de seguridad informática, evidencia de auditoría, papeles de trabajo, informe de auditoría pertinente a la Auditoría Informática.

Desde la perspectiva metodológica se utilizará el método empírico como es la observación directa de la Unidad de Gestión Tecnológica, cabe señalar que se aplicará el método deductivo para identificar los procesos que se desarrollan en la UGT y el método inductivo para identificar las actividades de los servidores y servidoras públicas; además las técnicas utilizadas son: entrevistas al personal del área objeto de estudio y encuestas dirigidas a los servidores y servidoras públicas, finalmente cabe mencionar la aplicación de la Norma Técnica de Control Interno (410 Tecnologías de la Información y Comunicación) establecida por la Contraloría General del Estado.

Desde la perspectiva académica la realización del presente trabajo de investigación se fundamenta en la aplicación de conocimientos que se han adquirido en el transcurso de la carrera de contabilidad y auditoría para llevar a cabo la Auditoría Informática, la misma que servirá de base para futuras investigaciones.

En cuanto a la justificación práctica para el desarrollo del presente trabajo de investigación se realizará el proceso de Auditoría Informática, para conocer el manejo y control de los recursos informáticos, con el propósito de presentar el informe de auditoría que contemple las conclusiones y recomendaciones que aporten a la toma de decisiones que mejoren las condiciones de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo.

1.3.OBJETIVOS

1.3.1. Objetivo General

Realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, para evaluar la seguridad de la información.

1.3.2. Objetivo Específicos

- Analizar los riesgos que inciden en la seguridad de la información de la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

- Identificar los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

- Presentar el informe al concluir el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES INVESTIGATIVOS

Al haber consultado varios trabajos de investigación referentes al tema de Auditoría Informática se detallan a continuación los siguientes autores con las conclusiones más notables:

En el repositorio digital UTC (UNIVERSIDAD TÉCNICA DE COTOPAXI):

Los autores Hidalgo, M. & Ortega, M. (2014) con el tema de investigación titulado como Aplicación de una auditoría informática a la seguridad física a los equipos de cómputo del GAD Municipal del Cantón Salcedo ubicado en la Provincia de Cotopaxi durante el periodo 2011. Universidad Técnica de Cotopaxi. Unidad Académica de Ciencias Administrativas y Humanísticas. Carrera de Contabilidad y Auditoría. Concluyeron que los departamentos que fueron evaluados, la seguridad física no contaban con el debido respaldo de artefactos que puedan controlar alguna catástrofe tales como incendios, inundaciones o terremotos lo que ocasione perdida de información; además los espacios físicos en donde funciona el área de informática no guarda seguridades de acceso, son reducidos y no mantienen un ambiente de temperatura y humedad adecuado, además no se definen sitios fuera de la entidad que permitan almacenar la información considerada critica, lo cual no garantiza la perpetuidad de los datos y su recuperación.

Este trabajo de titulación contribuyó en el análisis interno sobre el manejo de los equipos de cómputo y la toma de decisiones para solucionar las falencias encontradas en cuanto a la seguridad física de los equipos informáticos del GAD Municipal del Cantón Salcedo.

En el repositorio digital ESPOCH:

El autor Velin, J. (2016) con el tema denominado Auditoría Informática al Gobierno Autónomo Descentralizado Municipal de Pastaza, período 2014. Escuela Superior Politécnica de Chimborazo. Facultad de Administración de Empresas. Escuela de Contabilidad y Auditoría. Concluyó que mediante los procedimientos de auditoría realizados se determinó que no se cumplen con todas las Normas de Control Interno emitidas por la Contraloría General del Estado, siendo las más importantes la 410-15

Capacitación Informática, 410-01 Organización informática y 410-11 Plan de Contingencias. Además el Municipio posee una Unidad Informática que se encarga de regular, estandarizar, asegurar y generar la cobertura de servicios tecnológicos a todas las unidades de la entidad, pero no se ha elaborado un Plan de Contingencias que ayude a proteger la integridad de los activos informáticos, que permita mitigar los riesgos. Finalmente no se ha considerado en la capacitación al personal sobre el correcto manejo y las medidas de seguridad que se deben cumplir con los Activos de las TICs.

Este trabajo de titulación identificó el incumplimiento de las Normas Técnicas de Control Interno 410 (Tecnologías de la Información y Comunicación) con respecto a la capacitación y diseño de un plan de contingencias, falencias que se pusieron a consideración de la máxima autoridad del Gobierno Autónomo Descentralizado Municipal de Pastaza para salvaguardar los recursos tecnológicos y garantizar la integridad de la información.

La autora Lara, Y. (2017) con el tema denominado Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Guano, Provincia de Chimborazo, período 2015. Escuela Superior Politécnica de Chimborazo. Facultad de Administración de Empresas. Escuela de Contabilidad y Auditoría. Concluyó que no se cumplen con las Normas de Control Interno de la Contraloría General del Estado, debido al desinterés por parte de los directivos y falta de presupuesto para cumplir con lo que estipula específicamente la Norma 410 sobre Tecnologías de la información. Además la institución no posee un Plan de Contingencias que salvaguarde la integridad de los activos informáticos ni contrarreste el impacto de los posibles riesgos. Finalmente la dirección de Talento Humano no capacita al personal con respecto al manejo y seguridad de los equipos informáticos.

En este trabajo de titulación se evalúo la integridad, seguridad y disponibilidad de los activos informáticos, además se elaboraron indicadores de eficiencia, eficacia y seguridad del área informática, así detectó las áreas críticas y emitió las respectivas recomendaciones que salvaguarden la información y los activos informáticos institucionales.

2.2. FUNDAMENTACIÓN TEÓRICA

Para respaldar el presente trabajo de investigación se procede a citar fuentes de base científica para una mejor comprensión y desarrollo del mismo:

2.2.1. Definición de Auditoría

La auditoría es la revisión y análisis efectuado por un profesional en auditoría sobre la adecuada realización de las actividades y operaciones que se desarrollan en una empresa, para emitir una opinión con respecto a la razonabilidad de los resultados y el cumplimiento de las operaciones. (Muñoz, C., 2002, p. 11)

Mientras que para los autores Tapia, C., et al. (2016) la auditoría consiste en revisar los hechos y las operaciones, además el cumplimiento de las políticas y procedimientos, uso y aprovechamiento de los recursos.

Una vez analizadas las definiciones anteriores se concluye que la auditoría es la revisión detallada de la información y/o procesos, para obtener la evidencia que sustentará la opinión del auditor al presentar el informe respectivo al concluir con el proceso de auditoría.

2.2.2. Clasificación de la Auditoría

El autor Muñoz, C. (2002) propone la siguiente clasificación:

Tabla N° 1: Clasificación de la Auditoría

Según su lugar de origen	
Auditoria Externa	El profesional en auditoría que se encarga de la revisión de las actividades, operaciones y funciones es completamente ajeno a la empresa lo que le permite emitir una opinión libre e independiente.

Auditoría Interna	El profesional en auditoría tiene una relación de trabajo directa con la institución y se encarga de la evaluación interna del desempeño y cumplimiento de las actividades, operaciones y funciones de las áreas auditadas.
Según el área de aplicación	
Auditoría Financiera (Contable)	Comprende la revisión sistemática y crítica aplicada a las transacciones contables y financieras, Estados Financieros para determinar la razonabilidad, veracidad y confiabilidad sobre los mismos. Tiene como fin la emisión de un dictamen sobre las operaciones contables y financieras que contribuya a la toma de decisiones.
Auditoría Administrativa	Es la revisión de las actividades administrativas propias de una empresa, tiene como fin la evaluación del desempeño organizacional enfocados en la planificación, organización, dirección, evaluación y control.
Auditoría Operacional	Consiste en la evaluación sistemática a los procesos para determinar la suficiencia, eficiencia y eficacia en el desarrollo de las operaciones conjuntamente con las normas, lineamientos y políticas internas.
Auditoría Integral	Es una revisión sistemática y global de las actividades y operaciones, con el fin de evaluar el cumplimiento de la normativa vigente, determinar la eficiencia, eficacia y economía de los procedimientos y demostrar la razonabilidad de los Estados Financieros, que permitan al nivel institucional tomar las decisiones para alcanzar la misión, visión y objetivos institucionales.

Auditoría Gubernamental	Comprende una revisión sistemática y concreta de las actividades y operaciones de una entidad gubernamental, estatal o municipal; conjuntamente con las aplicaciones del presupuesto, programas y lineamientos que garanticen la transparencia en el manejo de los recursos públicos en bienestar de la sociedad.
Auditoría Informática	Es la revisión técnica orientada a evaluar el uso de los sistemas computacionales, software, instalaciones, mobiliario y otros componentes informáticos de una organización que garanticen información oportuna y precisa.

Fuente: Muñoz, C. **(**2002**)**. *Auditoría de Sistemas Computacionales.* México: Pearson Educación. (pp. 15, 19)
Elaboración: Autora

2.2.3. Definición de Auditoría Informática

A continuación se cita definiciones acerca de la auditoría informática

Para autores Piattini, M. & Del Peso, E. (2001) la auditoría informática consiste en recolectar y evaluar las evidencias que determinen si un sistema informático protege los activos y la información, además verifica el cumplimiento eficaz de los objetivos organizacionales y la correcta utilización de los recursos. Así este tipo de auditoría apoya a los objetivos propios de una auditoría como son: los objetivos de protección de los activos y la integridad de los datos y finalmente los objetivos de gestión para asegurar la eficiencia y eficacia de los activos.

Según los autores Tapia, C., et al. (2016) definen a la auditoría informática como la revisión y evaluación de los controles, sistemas y procesos de informática, así como uso eficiente y las medidas de seguridad que salvaguarden los equipos informáticos y posteriormente facilitar la toma de decisiones.

Una vez analizadas las definiciones anteriores se concluye que la auditoría informática es un examen sobre el manejo del software y hardware para salvaguardar la información y garantizar el uso eficiente de los equipos informáticos de una institución.

2.2.4. Control interno

El control interno comprende los parámetros y procedimientos necesarios para que la organización alcance las metas y objetivos planteados.

A continuación se presenta un cuadro comparativo entre los métodos de control interno como son: COSO I, II y III, COBIT 4.1 e ITIL:

Tabla N° 2: Métodos de Control Interno

MÉTODOS DE CONTROL INTERNO		CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
COSO Committee of Sponsoring Organization of the Treadway Commission (Comité de Organizaciones Patrocinadoras de la Comisión de Norma)	**COSO I 1992 Internal Control-Integrated Framework (Control Interno-Marco Integrado)**	Tiene 5 elementos • **Ambiente de Control** Son políticas y procedimientos que guian la actitud de los niveles de administración. • **Evaluación del Riesgo** Mecanismos para identificar riesgos. • **Actividades de Control** Políticas que respaldan las acciones para la identificación de los riesgos. • **Información y Comunicación** Registra e informa de las operaciones de la institucion. • **Monitoreo** Evaluación continua del desempeño del control interno.	• Efectividad y eficiencia en las operaciones. • Confiabilidad en la información financiera. • Cumplimiento de las leyes y normas vigentes. • Salvaguarda de los recursos institucionales. • Representa la base fundamental para crear los diferentes sistemas de control interno. **En Ecuador** La Contraloría General del Estado establece para las entidades que dispongan de recursos públicos, la utilización del marco integrado de control interno con los cinco componentes.	• Busca lograr los objetivos establecidos, pero no en todos los componentes. • Es útil para pocas empresas. • Todos los miembros de la organización deben saber a cerca de la funcionalidad de este sistema.

	COSO II 2004 Enterprise Risk Management -Integrated Framework (Gestión de Riesgo Empresarial-Marco Integrado)	Comprende 8 elementos que incluyen el análisis del riesgo para identificar, controlar y eliminar los riesgos identificados: • Ambiente interno • Establecimiento de objetivos • Identificación de eventos • Evaluación de riesgos • Actividades de control • Respuesta al riesgo • Información y comunicación • Monitoreo	• Ayuda a obtener una visión global del riesgo**.** • Pone en marcha los planes para la correcta gestión del riesgo. • La toma de decisiones es más certera. • Guía los objetivos claves para afrontar el riesgo. • Brinda soporte en la planificación y control interno organizacional.	• Consigue el cumplimiento de las actividades de acuerdo a lo planificado, sin embargo no alcanza el crecimiento organizacional. • Los lineamientos ante los riesgos se encuentran establecidos, pero los resultados dependen de la toma de decisiones.

	COSO III 2013 Internal Control-Integrated Framework (Contro Interno – Marco Integrado)	Establece los 5 componentes del COSO I, pero le añade 17 principios que se enfocan: • Compromiso con la integridad y los valores éticos. • Establecimiento de la estructura, líneas de autoridad y responsabilidad. • Evaluación de riesgos de fraude • Identificación y análisis de cambios importantes. • Selección y desarrollo de controles generales sobre tecnología. • Comunicación interna y externa. • Evaluaciones continuas o independientes.	• Contribuye a las actividades de planificación estratégica y control interno. • Promueve la gestión del riesgo en la cultura organizacional. • Este modelo de control interno surge ante la necesidad de obtener información fiable por parte de los usuarios internos y externos. • Los sistemas de gestión se adaptan al entorno organizacional. • Minimiza los riesgos y colabora en la consecución de objetivos. • Las líneas de información y comunicación son más eficaces.	• Requiere implementar un control interno eficiente. • El compromiso y responsabilidades deben ser asumidos por todos los miembros. • Es indispensable integrar los cinco componentes para alcanzar los objetivos institucionales.

COBIT 4.1 **Objetivos de Control para la Información y la Tecnología relacionada**	Es un modelo de procesos que se subdivide en 34 procesos considerando las áreas como: planear, construir, ejecutar y monitorear, ofreciendo una visualización clara de TI. Se debe considerar los siguientes dominios: **Planear y Organizar (PO):** Entrega solución y servicios. Se encuentran alineados los objetivos de TI con los objetivos del negocio. **Adquirir e Implementar (AI):** Establecer soluciones y las convierte en servicios. Nuevos proyectos generan soluciones para satisfacer el negocio. **Entregar y Dar Soporte (DS):** Recibe soluciones que son utilizadas por los usuarios. Se entrega servicios de TI de acuerdo a las prioridades del negocio. **Monitorear y Evaluar (ME):**	• Brindan buenas prácticas mediante un marco de dominios y procesos, con una estructura entendible y lógica. • Apoya al gobierno de TI, porque garantiza las TI están encaminadas a los objetivos del negocio, que los recursos de TI son usados correctamente. • Satisface las necesidades de los interesados internos y externos.	• Es necesario un estudio y dominio profundo. • Estan enfocadas en el control y menos en la ejecución. • Debe vincular a los usuarios y modelos de madurez para enlazar las metas organizacionales con las de TI. • La orientación a negocios es la parte fundamental de COBIT. • Se debe establecer

	Monitorea los procesos y garantiza que sigan la dirección establecida. Se mide el desempeño de TI para detectar problemas.		modelos de madurez, es decir, evaluar la situación de la organización.
ITIL **Information Techonology Infraestructure Library (Biblioteca de Infraestructura de Tecnologías de Información)**	• Describen un marco integrado por procesos que incluye las mejores prácticas para la gestión de los servicios de TI. • Resulta de la necesidad y exigencia de servicios informáticos de calidad. • Los procedimientos estandarizados se enfocan en la continuidad de los servicios de TI. • Se reconoce como un estándar global que resume a las mejores prácticas para el área de la gerencia de servicios de TI. • Su ciclo de vida comprende: Estrategia	• Se enfoca más en los procesos del negocio. • Facilita la comunicación con los usuarios. • Mejora la calidad de los servicios entregados al cliente acorde a las necesidades. • Aumenta la satisfacción del cliente y usuario final. • Mejora la productividad del negocio en cuanto a eficiencia y eficacia de los recursos. • Ayuda a los individuos sobre las prácticas que inducen a la mejora continua de los servicios para obtener mayores beneficios.	• La implementación de ITIL conlleva tiempo y mucho esfuerzo debido al cambio organizacional. • Puede no llegar a alcanzar los objetivos previstos. • Se denota la falta de comprensión de los procesos. • Puede aislar al

	Diseño Transición Operación Mejora continua	• Se adapta al área de servicio al cliente.	departamento de TI. • Demanda gran inversión para las herramientas de soporte, así como en personal y recursos.

Fuente:

Asociación Española para la calidad **(2018)**. *COSO*. Recuperado de https://www.aec.es/web/guest/centro-conocimiento/coso

Contraloría General del Estado **(2014)**. *Normas Técnicas de Control Interno*. Recuperado de: http://www.oas.org/juridico/pdfs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

IT Governance Institute **(2007)**. *COBIT 4.1*. Recuperado de: http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf

Matías, M**. (2017)**. *Marco Referencial ITIL: Ventajas y desventajas*. Recuperado de http://itilmmatiasc.blogspot.com/2017/05/ventajas-y-desventajas-de-itil.html

Elaboración: Autora

2.2.5. Tipos de Control Interno

El auditor debe considerar tres tipos de controles que se detallan a continuación:

- **Controles preventivos:** Se realizan este tipo de controles a fin de evitar un hecho que puede llegar a afectar las operaciones.
- **Controles detectivos:** Se realiza este tipo de controles para identificar errores u omisiones que no fueron posibles ser detectados con los controles preventivos.
- **Controles correctivos:** Este tipo de control consigue reestablecer la continuidad de las operaciones. (Piattini, M. & Del Peso, E., 2001)

2.2.6. Normas Técnicas de Control Interno

La Contraloría General del Estado (2014) instituye las Normas Técnicas de Control Interno que incluyen:

100 Normas Generales

Es responsabilidad de la máxima autoridad, dirección e instituciones públicas, establecer un control interno como un proceso integral que permita alcanzar la misión institucional y el cumplimiento de objetivos como: ayuda en la eficiencia, eficacia de las operaciones a través de los principios de ética, además garantiza la confiabilidad, integridad y oportunidad de la información, cumple con las disposiciones legales y normativa de la entidad conforme a lo que ofrece productos y servicios de calidad, finalmente ayuda a proteger el patrimonio público contra la irregularidad ilegal y uso inadecuado.

200 Ambiente de Control

El ambiente de control constituye un conjunto de circunstancias y conductas que guían las acciones de una entidad, para el correcto desarrollo de las actividades para determinar los riesgos. También es una relevancia para mejorar el sistema de información y las actividades de monitoreo.

300 Evaluación del Riesgo

En cuanto a la evaluación del riesgo se establecerán los mecanismos necesarios que permitan la identificación, análisis y tratamiento de los posibles riesgos a los cuales se encuentre expuesta la organización en la consecución de sus objetivos. Además se deben considerar factores externos como la economía, política, tecnología, sociedad y ambiental. Por otro lado se encuentran los factores internos que consideran la infraestructura, el personal, sistemas informáticos y los procesos propios de la organización. A través de un plan de mitigación de riesgos se establecen estrategias de gestión que identifiquen, valoren y erradiquen los riesgos, mediante el respectivo análisis se determina la afectación en la consecución de objetivos.

400 Actividades de Control

Con respecto a las actividades de control que involucra a toda la organización y sus funciones, comprenden acciones de control de detección y prevención en cuanto a la separación de los procedimientos para la aprobación y verificación de los recursos. La revisión y la ejecución de las transacciones con unas acciones correctivas en caso de desviaciones e incumplimientos. Estas actividades están acopladas a un plan y objetivos institucionales.

410 Tecnología de la información

410 – 01 Organización Informática

Las empresas del sector público para un mejor proceso tecnológico de la información, para garantizar la transparencia, control y la participación de la alta dirección, bajo la responsabilidad de una unidad, la misma que debe constar en el organigrama estructural en un nivel que le permita brindar apoyo y asesoría; además esta unidad debe participar en la toma de decisiones que genere cambios y mejoras tecnológicas. Se debe considerar que esta unidad es independiente con respecto de las áreas usuarias y debe cubrir los servicios de toda la organización.

410 – 02 Segregación de funciones

El personal de tecnología de la información y los usuarios de los sistemas de información ejercen sus funciones y responsabilidades asignadas con el fin de evitar funciones incompatibles.

410 – 03 Plan informático estratégico de tecnología

La elaboración e implementación de un plan informático estratégico está a cargo de la Unidad de Tecnología de la Información, para la correcta administración de los recursos tecnológicos, éste deberá estar alineado a las políticas públicas.

Los planes operativos y estratégicos de los sistemas de información, serán actualizados permanentemente, monitoreados y evaluados trimestralmente para comprobar su ejecución y la toma de medidas correctivas.

410 – 04 Políticas y procedimientos

La documentación y socialización de las políticas, estándares y otros procedimientos relacionados con la tecnología de la información y comunicación de la organización será responsabilidad de la Unidad de Tecnología de la Información.

Las políticas y procedimientos serán actualizados permanentemente y contendrá las tareas, responsables de la ejecución, procesos de excepción, así como su cumplimiento, control y sanción administrativa en caso de incumplimiento.

410 – 05 Modelo de información organizacional

En cuanto al modelo de información organizacional es definido por la Unidad de Tecnología de la Información para facilitar la creación, uso y compartición de la misma a fin de garantizar la disponibilidad, integridad, exactitud y seguridad de los procesos y procedimientos correspondientes.

410 – 06 Administración de proyectos tecnológicos

La elaboración y administración de los proyectos informáticos en todas sus etapas estará a cargo de la Unidad de Tecnología de la Información.

410 – 07 Desarrollo y adquisición de software aplicativo

La Unidad de tecnología ayuda a regular cada uno de los procesos para desarrollar las aplicaciones y la adquisición del software para considerar los lineamientos, metodologías y procedimientos como la adquisición de software, la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales, entre otros.

410 – 08 Adquisición de infraestructura tecnológica

La adquisición de infraestructura tecnológica será responsabilidad de la Unidad de Tecnología de Información que ayuda a definir y actualizar los aspectos tecnológicos de la entidad considerando los objetivos institucionales. Además se evaluan los riesgos tecnológicos, el costo y la vida útil de la inversión para futuras actualizaciones.

Para la adquisición de hardware se realizará un detalle de las características técnicas como: marcas, modelo, número de serie, capacidades, con la finalidad de los equipos para la adquisición de las fases contractuales.

410 – 09 Mantenimiento y control de la infraestructura tecnológica

El mantenimiento y control de la infraestructura tecnológica será definido y regulado por procedimientos establecidos por la Unidad de Tecnología de Información para garantizar el uso adecuado de la infraestructura tecnológica de la entidad.

410 – 10 Seguridad de tecnología de información

Se establecerán mecanismos que garanticen la protección de los recursos informáticos y la salvaguarda contra pérdidas y fugas de la información procesada mediante los sistemas informáticos, para lo cual se aplican medidas como: ubicación adecuada, control de acceso físico, obtención periódica de respaldos, también se aplican estándares para los datos que asegure su recuperación.

410 – 11 Plan de Contingencias

En el aspecto tecnológico implementa los planes de contingencia ayuda a describir las acciones para los procedimientos de información para los programas. Además el plan de recuperación de desastres comprenderá: actividades previas al desastre (bitácora de operaciones), las actividades durante el desastre (plan de emergencia, entrenamiento) y finalmente las actividades después del desastre. El plan de contingencias una vez aprobado será socializado a todo el personal responsable y posteriormente sometido a evaluaciones frecuentes, además se dará seguimiento al trabajo y procesamiento de la información.

410 – 12 Administración de soporte de tecnología de información

La Unidad de Tecnología de Información está encargada de definir, aprobar y difundir los procedimientos de las operaciones para facilitar una correcta administración del soporte tecnológico para garantizar la confidencialidad, integridad y disponibilidad de los recursos informáticos, así como la respuesta oportuna del servicio tecnológico. Considera la revisión periódica, estandarización en identificaciones, autenticación y autorización de usuarios y la administración de cuentas, y hacer frente a software malicioso y posibles virus informáticos.

410 – 13 Monitoreo y evaluación de los procesos y servicios

La Unidad de Tecnología de Información está encargada de definir y ejecutar los procedimientos y demás mecanismos para la satisfacción del cliente interno y externo, con el objetivo de supervisar la gestión realizada y la toma de acciones correctivas.

410 – 14 Sitio web, servicios de internet e intranet

La elaboración de normas, procedimientos e instructivos de instalación, configuración y utilización del servicio de internet, intranet, correo electrónico y sitio web institucional, está bajo la responsabilidad de la unidad de tecnología de información, acatando disposiciones legales, normativas y los requerimientos de los usuarios. También va a considerar el desarrollo y aplicaciones de web o móviles que automaticen los procesos o trámites de los ciudadanos en general.

410 – 15 Capacitación informática

El personal de la Unidad de Tecnología de Información conjuntamente con la Unidad de Talento Humano serán los responsables de las capacitaciones, de acuerdo al plan de capacitación informático. Este plan se dirige también a los usuarios de los sistemas informáticos, para satisfacer necesidades conforme a evaluar el desempeño y conocimientos.

410 – 16 Comité informático

La creación del comité institucional tomará en cuenta: el tamaño de la entidad, la interrelación con otras entidades, además planteará objetivos para la correcta toma de decisiones a fin de evaluar las políticas internas con respecto al sistema de información.

410 – 17 Firmas electrónicas

Las entidades del sector público deberán ajustar e incorporar los procedimientos a los medios técnicos para el uso de la firma electrónica con respecto a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su reglamento.

Para la verificación de la autenticidad de la firma electrónica se emplearán procesos automatizados de validación, es por ello que las instituciones públicas adoptarán y aplicarán estándares tecnológicos para firmas electrónicas, promulgadas por las entidades oficiales, de conformidad con los ámbitos competitivos y de acción. Además está enmarcado a políticas internas de manejo y archivo de información digital.

Una vez que el servidor público que posea un certificado de firma electrónica, cese sus actividades sea temporalmente o definitivamente procederá a solicitar la revocación del mismo y será cancelado inmediatamente, luego el dispositivo portable será devuelto mediante acta de entrega recepción para resguardar su validez y vigencia.

500 Información y Comunicación

El sistema de información y comunicación se encuentra constituido por métodos que permiten el registro, procesamiento, resumen e información de las actividades técnicas, administrativas y financieras de la entidad que servirá para tomar decisiones oportunamente.

500-01 Controles sobre sistemas de información

El uso de los sistemas automatizados en el procesamiento de la información concierne riesgos que la administración debe tomar en cuenta. Estos riesgos son cambios tecnológicos los mismos que deben ser controlados para garantizar la seguridad de la información.

500 – 02 Canales de comunicación abiertos

Los canales de comunicación abiertos son establecidos mediante políticas internas, que trasladan los aspectos internos y externos de la entidad de forma segura, oportuna y correctamente hacia los destinatarios.

600 Seguimiento

La máxima autoridad y el nivel directivo son los responsables de efectuar un seguimiento constante del ambiente interno y externo para mayor conocimiento y aplicación de medidas oportunas sobre las condiciones que afectan el desarrollo de las actividades y objetivos institucionales ya planificados. Se considera las evaluaciones periódicas como un factor primordial debido a que proporcionan una mayor eficacia de los componentes del control interno.

2.2.7. Normas de Auditoría Generalmente Aceptadas

El AICPA (American Institute of Certified Public Accountants) es una sigla en inglés que significa Instituto Americano de Contadores Públicos ha expuesto el marco de referencia en las siguientes 10 **normas de auditoría generalmente aceptadas**.

Gráfico N° 1: Normas de Auditoría Generalmente Aceptadas

Normas Generales	•**Capacidad Competitiva:** La auditoría debe llevarse a cabo por una persona profesional y capacitada técnicamente para la actividad. •**Independencia:** El auditor debe regirse a la independencia y a la ética profesional. • **Cuidado y Esmero:** El auditor debe tener el debido cuidado profesional en las fases de la auditoría como: planeación, ejecución y preparación del informe.
Normas de Trabajo de campo	•**Planeación y Supervisión:** El trabajo debe ser planeado adecuadamente y los miembros del equipo auditor deben ser supervisados apropiadamente. •**Estudio y Valoración del Control Interno:** Se lleva a cabo con las técnicas pertinentes y necesarias. •**Suficiencia:** El auditor debe obtener la evidencia suficiente, competente y veraz que constituya una base razonable para emitir una opinión.
Normas de Presentación del Informe	•**Aplicación de los PCGA:** El informe establece si la información está acorde con los principios de contabilidad generalmente aceptados PCGA. •**Consistencia:** Identificar si la información en el período actual mantiene consistencia con respecto al período anterior. •**Revelación Suficiente:**Se considera que las revelaciones sean razonables •**Opinión del Auditor:** La opinión puede ser expresada como: opinión sin salvedades, con salvedades, opinión negativa y abstención de opinar.

Fuente: Huatangare, D. **(2015)**. *Normas de Auditoría Generalmente Aceptadas*. Recuperado de: http://informe-nagas.blogspot.com/2015/09/normas-de-auditoria-generalmente.html

Elaboración: Autora

2.2.8. Proceso de Auditoría

La auditoría comprende una serie de fases que llegan a obtener un producto final como es el informe, a continuación se describe cada una de las fases del proceso de auditoría:

Planificación de Auditoría

La planificación comprende la primera fase del proceso de auditoría, como todo trabajo inicia con un grado de complejidad que requiere de una planificación sobre el desarrollo e implantación, es así como la planificación preliminar brinda una visión general del ambiente de la empresa, mientras que la planificación específica profundiza el trabajo a ser realizado.

Ejecución de Auditoría

En la fase de ejecución del trabajo de auditoría, se aplican las pruebas y metodologías necesarias para obtener las evidencias que deben tener dos características fundamentales para que sean válidas y pertinentes:

- Suficiencia
- Competencia

Para proceder a la comprobación y demostración de las evidencias, se obtienen mediante la base razonable de apoyo como son: la inspección, observación y confirmación de la información obtenida.

Comunicación de Resultados

Comprende la última fase del proceso de auditoría, que plasma en escrito el informe final que hace referencia a:

- **Consistencia:** El informe consta de las normas y principios de auditoría utilizados así como las excepciones de incumplimientos.
- **Revelación suficiente:** La información que proporciona el informe debe ser relevante y aportar algo nuevo que indique calidad y utilidad.

- **Opinión del auditor:** Al haber comentado sobre las técnicas utilizadas en la evaluación y ejecución del examen, el auditor emitirá una opinión sobre los resultados, acompañadas con las respectivas recomendaciones de mejora. (Chicano, E., 2014)

2.2.9. Evidencia de Auditoría

Para el autor Espino, G. (2014) la evidencia de la auditoría es toda información que utiliza el auditor para llegar a la conclusión en que se basa su opinión. (p. 6)

2.2.10. Tipos de evidencia

Los tipos más importantes de evidencia de auditoría son:

1. **Sistema de informe contable**
2. **Evidencia documental**

a) Evidencia creada fuera de la empresa y transmitida directamente a los auditores como los estados de cuenta bancaria.
b) Evidencia externa y conservada como por ejemplo: las facturas de proveedores, declaración de impuestos.
c) Evidencia creada y conservada por los clientes compo por ejemplo: cheques pagados.

3. **Declaraciones de terceros**

a) Confirmaciones
b) Cartas de abogados
c) Informes de peritos (especialistas)

4. **Evidencia física - Inventarios de mercancías y activos fijos**

a) Cálculos de depreciaciones y cálculos de ganancias por acciones
b) Interrelaciones de datos los costos de ventas, costos de producción;
c) Declaración de los clientes sean orales y escritas. (Espino, G., 2014)

2.2.11. Técnicas de Auditoría

De acuerdo a Alatrista, M. (2015) las técnicas de auditoría comprende los métodos prácticos aplicados por el auditor para alcanzar la informacion y comprobación necesaria para la emisión de la opinión.

2.2.12. Clasificación de las Técnicas de Auditoría

La clasificación de las técnicas de auditoría comprende:

1. Estudio General: Consiste en la apreciación y juicio de las características generales del entorno de la empresa, las cuentas y las operaciones, a través de los elementos más significativos que permitirán la elaboración de las conclusiones.

2. Análisis y Cálculo: Comprende el estudio de los elementos de un todo. Esta técnica es aplicada específicamaente al estudio de las cuentas de los Estados Financieros y consiste en volver a realizar las operaciones aritméticas de las cuentas y operaciones que se han realizado mediante cálculos sobre bases específicas.

3. Inspección: Consiste en la verificación física de las objetos, símbolo de las operaciones es aplicable a las cuentas cuyos saldos tienen una representación material como el efectivo, inventarios, activos fijos, etc.

4. Confirmación: Se refiere a validaciones realizadas por parte del auditor con respecto a la autenticidad de los saldos, hechos y operaciones pasadas.

5. Declaraciones y Certificaciones: Se refiere a la traducción formal de la técnica de la investigación, convirtiendo las afirmaciones recibidas en documentos escritos (declaraciones) y en algunas ocasiones serán certificadas por alguna autoridad competente (certificaciones).

6. Observación: Se refiere a la inspección es menos formal y se aplica en la observación directa de las operaciones para verificar su desarrollo normal. (Alatrista, M., 2015)

2.2.13. Documentación de la Auditoría o Papeles de Trabajo

Los papeles de trabajo representan un conjunto de registros que realiza y conserva el profesional en auditoría con respecto al trabajo realizado. Entre los ejemplos de los papeles de trabajo tenemos los programas de trabajo, memorándum, cartas de confirmación, declaraciones de la administración, extractos de documentos históricos de la entidad y comentarios obtenidos por el profesional en auditoría. (Espino, G., 2014)

Los papeles de trabajo son diseñados bajo los criterios y necesidades del auditor, considerando la revisión realizada en la empresa, el sistema de información a ser evaluado y los aspectos más relevantes. (Chicano, E., 2014)

De las definiciones anteriores se concluye que los papeles de trabajo constituyen una base elaborada sobre el trabajo del auditor que respaldan la opinión que posteriormente se comunica en el informe.

2.2.14. Utilización de los archivos

Según Chicano, E. (2014) la documentación del proceso de auditoría comprende dos tipos de archivos distintos:

- **Archivo Permanente o continuo:** Contiene los papeles de trabajo que son de utilidad para futuras auditorías. Para lo cual contiene los aspectos generales de la organización, leyes que amparan al sector al que pertenece la organización, estructura de las autoridades, organigrama organizacional, características de los equipos que componen el sistema de información, los respectivos manuales de instrucciones y utilización de los equipos.

- **Archivo Corriente:** También es llamada archivo de auditoría en curso, contiene los papeles de trabajo elaborados por el auditor durante todo el proceso de auditoría.

2.2.15. Metodología en Auditoría Informática

Actualmente los tipos de metodología más utilizados en Auditoría Informática son:

- R.O.A. (RISK ORIENTED APPROACH), diseñada por Arthur Andersen.
- CHECKLIST o Cuestionarios
- AUDITORÍA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; Paquete de seguridad RACF, etc.).

Las metodologías mencionadas se basan en la minimización de los riesgos, mediante la existencia y funcionalidad de los controles. La metodología más usada por su fácil utilización es la de CHECKLIST. (Piattini, M. & Del Peso, E.,2001)

2.2.16. Riesgo de Auditoría

Según Pallerola, J. & Monfort, E. (2014) el riesgo de auditoría comprende los aspectos cuantitativos y cualitativos, que pueden o no ser detectados por el auditor durante el examen. Todo riesgo que no es previsible, ante esto el auditor debe planificar la revisión de las áreas en las que podría suscitarse posibles riesgos y cuantificarlos para compararlos con la materialidad. La estimación de un riesgo debe acogerse al principio de prudencia y justificación que lo sustente.

Una vez analizada la definición anterior se concluye que el riesgo de auditoría comprende las fallas no detectadas durante el proceso de auditoría, ante las cuales la opinión del auditor es susceptible a cambios significativos.

2.2.16.1 Análisis del Riesgo

Según la autora Velázquez, A. (2011) para identificar los riesgos es necesario determinar un nivel en función de la seguridad como se puede observar a continuación:

Tabla N° 3: Análisis del Riesgo

Alto	Medio	Bajo
Si la amenaza representa un gran impacto en la institución.	Si la amenaza tiene un impacto parcial en las actividades de la institución.	Si la amenaza no tiene un impacto representativo en los procesos de la institución.

Fuente: Velázquez, A. **(**2011**)**. *Análisis del Riesgo*. Recuperado de: http://aplicaciondeseguridadinformatica.blogspot.com/2011/08/b-clasificacion-de-los-principales.html

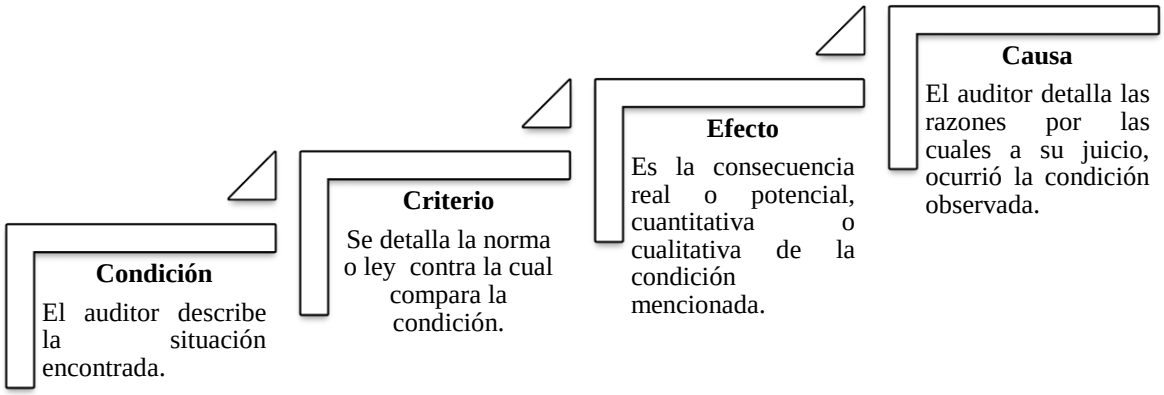
Elaboración: Autora

2.2.17. Hallazgo de Auditoría

Para Marulanda, L. (2016) el hallazgo de auditoría es una narración explicativa y lógica de los hechos detectados en el examen de auditoría, referente a deficiencias, desviaciones, irreguralidades, errores, debilidades, fortalezas y/o necesidades de cambio. (p. 6)

Los elementos del hallazgo son cuatro y se describen en el gráfico N° 2:

Gráfico N° 2: Atributos del Hallazgo



Fuente: Marulanda, L. (2016). *Hallazgo de Auditoría.* Recuperado de: https://www.contraloriabga.gov.co/files/HALLAZGOS_LEMT.pdf

Elaboración: Autora

2.2.18. Informe de Auditoría

El informe de auditoría es el documento escrito que plasma los resultados que se obtuvieron durante el examen de auditoría, conjuntamente con las conclusiones y recomendaciones emitidas por el auditor. La correcta elaboración del informe es fundamental, ya que se da a conocer a la organización la situación para que la máxima autoridad tome las medidas necesarias. (Chicano, E., 2014)

2.2.19. Tipos de Opinión

El informe contiene los siguientes tipos de opinión:

- **Opinión favorable:** Este tipo de opinión es limpia sin salvedades, resulta de un trabajo realizado sin limitaciones de alcance e incertidumbres.
- **Opinión con salvedades:** Representa salvedades cuando son significativas en relación a los objetivos de la auditoría, puede suceder si hay limitaciones en el alcance del trabajo, si existe incertidumbres que no permitan una previsión razonable, si existen irregularidades significativas y el incumplimiento de la ley.

- **Opinión desfavorable:** También conocida como opinión adversa se aplica en casos de identificación de irregularidades, incumplimiento de la normativa legal que afecte significativamente los objetivos de la auditoría informática planteados.
- **Opinión denegada:** Tiene su origen en las limitaciones del alcance de la auditoría, incertidumbres significativas que impidan al auditor emitir una opinión, irregularidades, incumplimiento de la normativa legal y profesional. (Piattini, M. & Del Peso, E., 2001)

2.2.20. Seguridad Informática

La seguridad informática procura que los recursos informáticos (material informático y programas) sean utilizados de la manera en la que fueron planificados, además asegurar el acceso a la información y que la modificación sea sólo realizada por personas autorizadas y dentro de los límites de su autorización. (Costas, J., 2014)

2.2.21. Principios de la Seguridad Informática

Para el autor Costas, J. (2014) los principios de la Seguridad Informática son:

Confidencialidad: Es la cualidad que poseen los documentos o archivos, para que sean entendidos de forma comprensible por una persona autorizada o para quien va dirigido.

Integridad: Se considera esta cualidad cuando los documentos o archivos no han sido alterados o manipulados, los mismos pueden ser comprobados en el documento original.

Disponibilidad: Se refiere a la capacidad de un servicio, sean datos o sistemas, al ser accesibles y puedan ser utilizados por los usuarios autorizados cuando lo necesiten.

2.2.22. Elementos vulnerables en un sistema informático

Son tres los elementos que deben ser protegidos en un sistema informático: El software, el hardware y los datos. El hardware comprende todos los elementos físicos de un sistema informático como CPU, cableado, medios de almacenamiento secundario (disquetes, CD-ROM, o tarjetas de red).

El software comprende el conjunto de programas lógicos que hacen funcionar al hardware como los sistemas operativos, aplicaciones, y por datos se entiende el conjunto de información lógica que es manejada por el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. (Costas, J., 2014)

2.2.23. Amenazas a un sistema informático

Las amenazas que pueden afectar a un sistema informático provienen de un hacker, un programa descargado gratis e incluso por una contraseña débil. A continuación se detallan las amenazas a un sistema informático:

- **Personas:** Las personas pueden constituir un fuente de riesgo para el sistema informático, existen atacantes pasivos que sólo miran la información sin alterarla, sin embargo también están los atacantes activos que buscan dañar la información.

  Se considera que los empleados o funcionarios pueden afectar la seguridad de los equipos, también están los ex – empleados que aun ante el cese de las actividades laborales mantienen la cuenta de usuario institucional para utilizarla a su favor, también están los curiosos que solo desean obtener información personal, un hacker describe una persona experta en programación que busca acceder a la red con malas intenciones pero no siempre es así. Mientras que un cracker describe una persona que intenta conseguir acceso no autorizado a la red con el fin de beneficiarse mediante intenciones maliciosas.
- **Amenazas lógicas:** Aquí se encuentran los programas o software maliciosos que pueden causar daños irreparables, en ocasiones, a los sistemas informáticos. A continuación se detallan algunos de ellos:

- **Bombas Lógicas:** Son partes de códigos de software que son activadas inesperadamente para causar perjuicios.
- **Canales cubiertos:** Constituyen canales de comunicación que permiten la transferencia de información hacia otros sistemas que no están autorizados para recibir dicha información.

- **Virus:** Formado por una secuencia de códigos que se introduce en un fichero ejecutable, al ser ejecutado, el virus (huésped) también se ejecuta, e insertándose en otros programas. Pueden afectar más a los sistemas operativos como Windows, mientras que para el sistema Linux no es un problema de seguridad grave.
- **Gusanos:** Software capaz de ejecutarse y propagarse así mismo a través de las redes, portando virus que provocan graves daños a los sistemas informáticos.
- **Caballos de Troya:** Son instrucciones escondidas en un software que aparece cuando el usuario realiza determinadas tareas, también se le conoce como troyano, pues oculta su apariencia, viendose inofensivo a primera vista.
- **Programas conejo o bacterias:** Son programas que no tienen utilidad alguna, se reproducen hasta acabar con la memoria del procesador y disco duro.

- **Amenazas físicas:** Las amenazas que pueden afectar a la seguridad y al funcionamiento de los sistemas informáticos son:

- Robos, sabotajes y destrucción de los sistemas informáticos.
- Cortes, subidas y bajadas bruscas del suministro eléctrico.
- Condiciones ambientales como la humedad excesiva o altas temperaturas que alteren el comportamiento normal de los recursos informáticos.
- Catástrofes, que pueden afectar debido a la ubicación geográfica, se mencionan los terremotos, inundaciones, incendios, humo o ceniza volcánica. (Costas, J., 2014)

Además Roa, J. (2013) señala que se debe considerar los siguientes factores de riesgo a la seguridad informática:

- **Desastres naturales** (como incendios, inundaciones, hundimientos, terremotos): Se debe tomar en cuenta al momento de ubicar el centro de proceso de datos (CPD), en donde se alojan los principales servidores de la institución; pero, aunque se posea un sistema de extinción de incendios se debe tener un segundo CPD para evitar la paralización de actividades.
- **Robos:** Se debe proteger el acceso a la sala del CPD mediante diversas medidas de seguridad como: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.

- **Fallos de suministro:** Es necesario prepararse para las ocasiones en que fallen los suministros de energía, una segunda conexión a Internet como línea de backup —incluso una solución inalámbrica— para proteger ante un corte.

2.2.24. Mecanismos de seguridad

Los mecanismos o medidas de seguridad a ser aplicadas son los siguientes:

- **Activas:** Son aquellas medidas que evitan daños a los sistemas informáticos a través del empleo de contraseñas adecuadas para el acceso a sistemas y aplicaciones, encriptación de los datos, filtración de conexiones en redes, uso de software específico de seguridad informática a fin de evitar el denominado malware.
- **Pasivas:** Son aquellas que minimizan el impacto y los efectos causados por accidentes a través del uso de hardware adecuado, protección física, eléctrica y ambiental, es imprescindible la realización de copias de seguridad para recuperar la información. (Costas, J., 2014)

2.2.25. Seguridad Física

De acuerdo a los autores Escrivá, G., et al. (2013), la seguridad física consiste en un conjunto de medidas preventivas y de detección a fin de evitar daños físicos a los sistemas informáticos y proteger los datos que almacena.

La seguridad física hace referencia a los mecanismos para la aplicación de barreras físicas y procedimientos de control, que protejan el hardware y los medios de almacenamiento de la información.

También se puede distinguir los tipos de seguridad física de las instalaciones:

- **Seguridad Física Interna:** Este tipo seguridad incluye: control de acceso mediante cámaras de seguridad, detectores de movimiento y tarjetas de identificación.
- **Seguridad Física Externa:** Se refiere a las instalaciones de los servidores así como el despliegue de la red y cableado. (Costas, J., 2014)

2.2.26. Elementos de la seguridad física

Instalaciones físicas: Para la fijación de medidas preventivas que salvaguarden los equipos informáticos se debe considerar el lugar y ubicación de los mismos.

Instalaciones eléctricas: Los equipos informáticos necesitan de energía eléctrica para funcionar, la misma que llega a través de conexiones, si la instalacion es defectuosa puede provocar graves daños. Se debe adoptar las siguientes medidas preventivas:

- **Protección eléctrica adecuada:** Es necesario que los enchufes tengan tomas de tierra y la corriente sea estable para evitar picos de tensión.
- **Mantenimiento del suministro eléctrico:** Debido a las anomalías de la corriente eléctrica, como los apagones, caídas y picos de tensión, sobrevoltajes, es necesario desarrollar Sistemas de Alimentación Ininterrumpida (SAI) o como se le conoce en inglés Uninterrupted Power Supply (UPS) que proporcione alimentación a los equipos en caso de cortes de energía eléctrica, así dan tiempo a los equipos que se apaguen correctamente y no se pierda información.
- **Instalación de una red adecuada:** Al estar conectados los equipos a una red local, se debe proteger la red de accesos físicos no deseados. Además se debe controlar que el cableado sea el correcto.
- **Control de acceso:** Se debe controlar el acceso al lugar donde se encuentra el ordenador sea una oficina o una unidad especializada. Esta medida se aplicará mediante el establecimiento de claves o registros de entrada y salida.
- **Protección frente a incendios:** Se emplean sistemas de prevención mediante la instalación de detectores de humo y alarmas. En cuanto a los sistemas de protección, son aquellos que ponen en marcha acciones en caso de incendio, como barreras que aislen el incendio, el entrenamiento y aplicación de evacuaciones y uso de salidas de emergencia, así como el uso de extintores, en caso de incendios dentro de la oficina, se utilizarán los extintores de clase C, es decir, de polvo seco polivalente o CO2. Nunca apagar un incendio con agua porque se corre el riesgo de sufrir una descarga eléctrica. (Escrivá, G., et al., 2013)

Según Tamayo, J. & Tamayo, A. (s/f) otros aspectos a considerar dentro de la seguridad fisica que tienen una importancia significativa en cuanto a la integridad, disponibilidad y confidencialidad de la información son los siguientes:

- **BACK– UPS:** Consiste en guardar copias de los archivos en lugares externos al área de informática y en instalaciones de alta seguridad. Estas copias deben ser obtenidas al menos cada dos meses y deben ser controladas minuciosamente.

- **Pólizas – Seguros:** Debe cubrir el total del valor comercial del hardware y software, deben estar permanentemente actualizados, así también se debe revisar la fecha de vencimiento a fin de evitar expiraciones inesperadas. Además se debe establecer un valor determinado como fianza al personal que labore en el área de sistemas.

- **Plan de contingencias:** El plan debe cubrir el hardware, software, documentos, recurso humano y soporte logístico, éste debe ser socializado a todos los funcionarios y coordinar las acciones en caso de alguna contingencia, a través de simulacros, también debe ser actualizado continuamente por un comité formalmente constituido.

2.2.27. Centro de Proceso de Datos

El Centro de Proceso de Datos (CPD) en su denominación inglesa Data Center, comprende los sistemas informáticos que requieren de servidores con varios procesadores y unidades de disco, sistemas de comunicación avanzados con varios routers, switches, equipos de alimentación redundantes, dispositivos de copias de seguridad. Estos equipos se encuentran trabajando a una temperatura ambiente de entre 17° y 19° C, generan mucho ruido por lo que deben estar confinados en un lugar adaptado. Este CPD trabajo ininterrumpidamente las 24 horas de los 365 días del año. (Escrivá, G., et al., 2013)

Requisitos que debe poseer un Centro de Proceso de Datos

- **Disponibilidad y monitorización:** Un CPD proporciona disponibilidad, accesibilidad y confianza las 24 horas durante los 365 días del año.
- **Fiabilidad infalible (5 nueves):** El nivel de disponibilidad de 99,999%, es decir, una hora de no disponibilidad al año. Por lo que los CPD deben contar con redes y equipos altamente robustos y comprobados.
- **Seguridad, redundacia y diversificación:** Cuenta con almacenamiento exterior de datos, tomas eléctricas independientes, equilibrio de cargas con los UPS o SAI.
- **Control Ambiental/prevención de incendios:** Control de la temperatura, humedad, inundación, electricidad y el control de acceso físico.
- **Acceso a Internet y conectividad a redes de áreas extensa WAN para conectividad a Internet:** Los CPD deben ser mejorados en cuanto a equipos, estándares y ancho de banda sin dejar de lado la fiabilidad. (Costas, J., 2014)

2.2.28. Estándares de Seguridad para Data Center

2.2.28.1. Estándar TIA 942

El estándar TIA 942 representa una guía para los diseñadores e instaladores de centros de datos (Data Centers), debido a que provee una serie de lineamientos para la instalación de sus infraestructuras.

En el año 2005 se aprobó el estándar TIA 942, ANSI-TIA (American National Standards Institute – Telecomunications Industry Association), define los tipos de centros en grupos denominados TIER, pues indican el nivel de fiabilidad en función del nivel de disponibilidad.

Los centros de datos deben ser diseñados para ofrecer ventajas con respecto a: Nomenclatura estándar, funcionamiento a prueba de fallos, máxima protección para hacer frente a los agentes externos, garantizar fiabilidad a largo plazo y sobre todo mayores capacidades de expansión.

La infraestructura de soporte de un Data Center estará compuesta por cuatro subsistemas:

- **Telecomunicaciones:** Se refiere a la instalación del cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y alimentación redundantes.
- **Arquitectura:** Con respecto a la parte física debido a que selecciona la ubicación, tipo de construcción, protección ignífuga como barreras de vapor, techos y pisos, áreas de oficina, salas de UPS y baterías, sala de generador, control de acceso, NOC (Network Operations Center – Centro Operativo).
- **Sistema eléctrico:** Establece el número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, conexión a tierra, generadores, sistemas de transferencia.
- **Sistema mecánico:** Confiere el sistema de climatización, presión positiva, tuberías y drenajes, detección de incendios y de líquidos.

De acuerdo al estándar, un CPD deberá incluir varias áreas funcionales:

- Una o varias entradas al centro.
- Área de distribución principal.
- Una o varias áreas de distribución principal.
- Áreas de distribución horizontal.
- Área de equipo de distribución.
- Cableado horizontal.

TIER

El nivel de fiabilidad de un CPD, se muestra en cuatro niveles, llamados TIER, con respecto a la redundancia. A mayor número de TIER, mayor disponibilidad, lo que significa mayores costos de construcción y mantenimiento.

Tabla N° 4: Niveles de fiabilidad

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,67%	0,33%	28,82 horas
TIER II	99,74%	0,25%	22,68 horas
TIER III	99,982%	0,02%	1,57 horas
TIER IV	99,999% - 100%	0,01%	52,56 minutos

Fuente: Grupo Confitel Andino **(**2014**)**. *Niveles de fiabilidad*. Recuperado de: https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

Elaboración: Autora

TIER I-NIVEL 1(BÁSICO)

- Disponibilidad del 99,671 %.
- Sensible a las interrupciones, planificadas o no.
- Un solo paso de corriente y distribución de aire acondicionado, sin componentes redundantes.
- Sin exigencias de piso elevado.
- Generador independiente.
- Plazo de implementación: 3 meses.
- Tiempo de inactividad anual: 28,82 horas.
- Debe cerrarse completamente para realizar mantenimiento preventivo.

TIER II- NIVEL 2 (COMPONENTES REDUNDANTES)

- Disponibilidad del 99,741 %.
- Menor sensibilidad a las interrupciones.
- Un solo paso de corriente y distribución de aire acondicionado, con un componente redundante. Además incluye piso elevado, UPS y generador.
- Plazo de implementación: 3 meses a 6 meses
- Tiempo de inactividad anual: 22,0 horas.
- El mantenimiento de la alimentación y otras partes de la infraestructura requieren de un cierre de procesamiento.

TIER III- NIVEL III (MANTENIMIENTO CONCURRENTE)

- Disponibilidad 99,982 %.
- Interrupciones planificadas sin interrupción de funcionamiento, pero posibilidad de problemas en las no previstas.
- Múltiples accesos de energía y refrigeración, por un solo encaminamiento activo. Incluye componentes redundantes (N+1).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: 1,6 horas.

TIER IV- NIVEL IV (TOLERANTE A ERRORES)

- 99,999 % de disponibilidad.
- Interrupciones planificadas sin interrupción de funcionamiento de los datos críticos. Posibilidad de sostener un caso de improviso sin daños críticos.
- Múltiples pasos de corriente y rutas de enfriamiento. Incluye componentes redundantes (2(N+1))- 2 UPS cada uno con redundancia (N+1).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: 0,4 horas.

(Grupo Confitel Andino, 2014)

2.2.28.2. Norma ISO 27001

ISO 27001 es una norma internacional establecida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa. La última revisión se denomina ISO/IEC 27001:2013.

ISO 27001 es una norma que se adapta a cualquier tipo de organización sea pública o privada. El pilar fundamental de la norma es la protección de la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace evaluando el riesgo y el tratamiento del mismo para proceder a mitigarlos.

Gráfico N° 3: Estructura ISO 27001

Fuente: Advisera Expert Solutions Ltd **(**s/f**)**. *Estructura ISO 27001*. Recuperdo de: https://advisera.com/27001academy/es/que-es-iso-27001/

Elaboración: Autora

Las medidas de seguridad a ser implementadas se formulan mediante políticas, procedimientos y la implementación técnica de software y equipos de una forma segura. Además se establece la redacción de documentos para prevenir alteraciones a la seguridad. Es así como la ISO 27001 detalla los elementos que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI), la misma que contempla la gestión de procesos, de recursos humanos, protección jurídica y física. (Advisera Expert Solutions Ltd., s/f)

2.2.29. Seguridad Lógica

La seguridad lógica comprende el conjunto de mecanismos que protegen los datos y las aplicaciones informáticas, limita que el acceso a la información sea solo para las personas autorizadas. (Escrivá, G., et al., 2013)

2.2.30. Niveles de Seguridad Lógica

De acuerdo al sitio web Segu.Info Seguridad de la Información (2009) los niveles de seguridad lógica son los siguientes considerando que cada nivel depende de los niveles ya definidos como el subnivel B2 que comprende los subniveles B1, C2, C1 y nivel D.

- **Nivel D:** Tiene una división y está reservada para sistemas evaluados que no cumplen con especificaciones de seguridad, como sistemas no confiables, inexistencia de protección de hardware, sistema operativo inestable, no hay una autenticación de usuarios. Los sistemas operativos de este nivel son MS-DOS y System 7.0 de Macintosh.
- **Nivel C1: Protección Discrecional:** Requiere la identificación y autentificación de usuarios para acceder a la información distinguiendo entre usuarios y administrador, los mismos que deben manejar su información de forma responsable y confidencial para ejecutar sus acciones sobre el sistema.
- **Nivel C2: Protección de Acceso Controlado:** El subnivel se diseñó ante las debilidades del nivel C1, crea un ambiente de acceso controlado, mediante la restricción que los usuarios ejecuten ciertos comandos o accedan a archivos confidenciales. Este nivel C2 permite llevar mejor la cuenta de las tareas ligadas a la administración del sistema, pues cada usuario ejecuta su trabajo.
- **Nivel B1: Seguridad Etiquetada:** Este subnivel es el primero que cuenta con el nivel B, el cual soporta seguridad multinivel, es decir secreta y ultrasecreta, mediante el establecimiento de control de acceso obligatorio, pues el dueño del archivo no puede modificar los permisos de un objeto del sistema (usuario, datos), pues se le asigna una etiqueta con un nivel de seguridad jerárquico sea alto, secreto o reservado, adicionalmente con categorías como nóminas, ventas, etc. Los usuarios den obtener un permiso expreso para acceder al objeto.
- **Nivel B2: Protección Estructurada:** Alude a un objeto más elevado de seguridad en comunicación con otro objeto de nivel inferior. El sistema alerta a los usuarios si las condiciones de accesibilidad y seguridad son modificadas, y el administrador fija canales de almacenamiento y ancho de banda para la utilización de los usuarios.

- **Nivel B3: Dominios de Seguridad:** Refuerza los dominios mediante la instalación del hardware como la administración de memoria para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Un monitor se encarga de permitir o denegar las políticas de acceso. Cada usuario tiene asignado un lugar y objeto a los que puede acceder.
- **Nivel A: Protección Verificada:** Comprende el nivel más elevado, pues incluye un proceso de diseño, control y verificación a través de métodos matemáticos para asegurar todos los procesos de un usuario sobre el sistema. Para alcanzar este nivel todos los niveles inferiores deben incluirse, además el hardware y el software son protegidos con infiltraciones ante traslados o movimientos del equipamiento.

2.2.31. Medidas de Seguridad Lógica

Las medidas de seguridad lógica son las siguientes:

- **Autenticación de usuarios:** Al asignar un usuario y contraseña, el sistema evita los accesos indebidos.
- **Listas de control de acceso:** Mecanismos para controlar que los usuarios realicen alguna actividad ajena en los recursos del sistema operativo.
- **Criptografía:** Es la técnica que transforma un mensaje legible en otro cifrado o ilegible para evitar que personas no autorizadas accedan a la información.
- **Acceso al sistema operativo y aplicaciones:** Al encender los equipos se debe crear la primera barrera lógica que impida el acceso a la información, las cuentas de usuario permiten restringir operaciones en el sistema informático. Se debe establecer una contraseña. La misma que debe contener una combinación de símbolos como números, letros y signos, considerar que debe tener al menos 14 caracteres.

  Se considera las amenazas a las contraseñas,si la contraseña no es suficientemente robusta será fácilmente descifrada. La inclusión de cifras, números y otros caracteres hacen que sea más fuerte, los sistemas establecen restricciones que obligan a los usuarios a ingresar contraseñas que le brinden una seguridad alta. Mediante la utilización de sniffers, que constituyen programas que registran las actividades en un equipo informático pueden ser interceptados para obtener las contraseñas. Además está

el uso de Keyloggers cuyo fin es capturar las pulsaciones en el teclado para descifrar las contraseñas. Otro método utilizado son los ataques por fuerza bruta que consiste en probar diversas combinaciones de caracteres hasta hallar la clave de acceso. Finalmente estan los ataques por ingeniería social que no es más que el engaño a los usuarios mediante la suplantación de identidades como amigos, empleados de entidades bancarias o técnicos profesionales en áreas específicas.

- **Acceso a aplicaciones por internet:** El uso de internet forma parte de la vida cotidiana es por esta razón que se debe tomar como medida de seguridad el bloqueo de páginas que soliciten información confidencial del usuario. Además se debe mantener actualizado el antivirus, se debe desconfiar de los sitios web que regenera una contraseña olvidada, evitar acceder desde ordenadores públicos, redes wifi abiertas, recordar cerrar la sesión correctamente a través del vínculo Salir o Cerrar Sesión. Finalmente para acceder a las páginas web y verificar si es fiable o no, es imprescindible fijarse en la barra de navegación que la dirección comience por https (hyper text transfer protocol secure) lo que significa que la conexión es segura, así como la aparición de un candado cerrado que es indicativo que la conexión es cifrada y al hacer doble clic aparece el certificado de identidad de la institución. (Escrivá, G., et al., 2013)

2.3.MARCO CONCEPTUAL

Auditor: Persona natural o jurídica que se dedica a realizar auditorías.

Backbone: Engloba conexiones de varios routers interconectados a nivel mundial.

Back-up: Copia de seguridad de uno o más archivos informáticos con el fin de prevenir pérdidas de información.

Cracker: Persona que utiliza sus conocimientos de informático para fines maliciosos.

Cable de Red: Cordón con conectores para los diferentes equipos informáticos.

Conexión a Tierra: Desviación de la corriente a tierra.

Contraseña: Autenticación de usuarios creada a base de caracteres alfanuméricos.

Encriptación: Consiste en el proceso que vuelve ilegible la información.

Hacker: Persona que manipula ilícitamente los sistemas informáticos para extraer información secreta. También se refiere a pirata informático.

Hardware: Conjunto de elementos físicos de un sistema informático.

Índice de Auditoría: Compendio que facilita el archivo y organización de los papeles de trabajo.

Informática: Conjunto de conocimientos técnicos sobre el tratamiento automático de la información a través del uso de ordenadores.

Internet: Red informática de nivel mundial que transmite información a través de una línea telefónica.

Intranet: Red informática interna de una institución, que conecta a varias computadoras al servicio web.

Malware: Software maliciosa que causa daño a los sistemas informáticos.

Marcas de Auditoría: Signos que utiliza el auditor en los papeles de trabajo para señalar la debilidad encontrada.

Materialidad en Auditoría: También conocida como importancia relativa denota las fallas u omisiones identificadas en el proceso de auditoría.

Programa de Auditoría: Documento escrito que enlista los procedimientos a ser efectuados en el proceso de auditoría.

Rack: Estructura que sostiene un equipo tecnológico.

Red: Conjunto de cables, vías de comunicación que se encuentran o cruzan en diversos puntos que sirven para transmisión.

Red LAN: Red de área local.

Riesgo inherente: Posibilidad de errores o irregularidades en la información financiera, administrativa y operativa antes de haber aplicado los controles internos de la organización.

Riesgo de detección: Ocurre cuando los procedimientos de auditoría no son suficientes para encontrar errores o irregularidades.

Riesgo de control: Probabilidad de que los controles internos establecidos no puedan prevenir los errores de forma oportuna.

Router: Dispositivo enrutador de conectividad de redes.

Sistema Informático: Conjunto de procesos para almacenar información mediante la interrelación del hardware, software y talento humano.

Software: Es la parte lógica que comprende el conjunto de programas para la realización de tareas.

Virus Informático: Programa que afecta totalmente o parcialmente un computador.

Sniffer: Usado por una persona maliciosa, puede llegar a hurtar información a través de la red local.

2.4. IDEA A DEFENDER

La Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, evaluará la seguridad de la información.

2.5. VARIABLES

2.5.1. VARIABLE INDEPENDIENTE

Auditoría Informática

2.5.2. VARIABLE DEPENDIENTE

Seguridad de la información.

CAPITULO III: MARCO METODOLÓGICO

3.1. MODALIDAD DE LA INVESTIGACIÓN

La investigación se sustentó en el enfoque cualitativo, nivel explicativo y exploratorio, porque acumula información mediante descripciones y observaciones. Además se consideró el enfoque cuantitativo, mediante el uso de modelos matemáticos y herramientas estadísticas para generar un análisis a partir de los datos recolectados y evidenciar la problemática planteada.

3.2.TIPOS DE INVESTIGACIÓN

Los tipos de investigación empleados fueron:

3.2.1. Investigación Descriptiva

La aplicación de este tipo de investigación ayudó a describir las observaciones realizadas sobre la situación de la Unidad objeto de estudio.

3.2.2. Investigación de Campo

La utilización de este tipo de investigación permitió estudiar la situación actual de la Unidad objeto de estudio.

3.2.3. Investigación Documental

La investigación documental consistió en la búsqueda de información en documentos como libros, artículos, ensayos y las Normas de Control Interno, que contribuyan al desarrollo del presente trabajo de investigación.

3.3.MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.3.1. Métodos de Investigación

Método deductivo

Este método parte de lo general a lo específico, la aplicación parte del cumplimiento de la Norma Técnica de Control Interno establecida por la Contraloría General del Estado.

Método inductivo

Este método analiza las partes para llegar a un todo, justificando su aplicación en el cumplimiento de políticas institucionales, que permiten el desarrollo de las actividades y procesos de la Unidad objeto de estudio.

Método Analítico

Este método de investigación identifica los procesos y actividades que se realizan en la Unidad objeto de estudio para procesar los datos y brindar información oportuna.

Método Sintético

Este método resume las funciones que cumple la Unidad objeto de estudio para contribuir al proceso de gestión de tecnología de la información y comunicación.

3.3.2. Técnicas de Investigación

Observación Directa

Esta técnica se aplicó mediante visitas a las instalaciones de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo, para recabar la información que condujo el desarrollo del presente trabajo de investigación.

Entrevistas

Esta técnica fue viable mediante el diálogo con el personal encargado de la Unidad objeto de estudio para obtener la información necesaria.

Encuestas

Se aplicó esta técnica mediante una serie de preguntas para conocer las opiniones y actitudes de los funcionarios de la institución sobre el uso de equipos informáticos y la aplicación de políticas internas.

3.3.3. Instrumentos de Investigación

Guía de observación

Este instrumento de investigación se utilizó para el desarrollo del presente trabajo y fue utilizado para plantear la problemática.

Guía de entrevista

Este instrumento constituyó una fuente de información directa a través de preguntas abiertas y cerradas dirigidas al Jefe y Técnicos profesionales encargados de la Unidad objeto de estudio.

Guía de encuestas

Este instrumento comprendió un conjunto de preguntas cerradas dirigidas al personal de la Unidad objeto de estudio; mientras que, para los funcionarios de la institución se aplicó una encuesta usando la Escala de Likert, para recolectar información que posteriormente fue organizada y analizada para corroborar la realización del presente trabajo de investigación.

Documentos

Se constituyen documentos los papeles de trabajo elaborados por el auditor.

3.4. POBLACIÓN Y MUESTRA

De acuerdo a la información publicada en el sitio web del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo (2018), existen 278 empleados laborando actualmente en la institución como se puede apreciar a continuación:

Tabla N° 5: Personal del GAD Municipal del Cantón San Pedro de Pelileo

UNIDAD	NÚMERO DE PERSONAS	PORCENTAJE
Alcaldía	1	0%
Concejo Cantonal	7	3%
Secretaria General	4	1%
Agua Potable	26	9%
Asesoría Jurídica	3	1%
Auditoría Interna	2	1%
Avalúos y Catastros	15	5%
Administrativo	21	8%
Administrativo (Gestión Tecnológica)	3	1%
Desarrollo de la Comunidad	29	10%
Financiero	18	6%
Obras Públicas	51	18%
Orden y Control	4	1%
Planificación	13	5%
Registro de la Propiedad	6	2%
Servicios Públicos	72	26%
Administración de Justicia	3	1%
Total	**278**	100%

Fuente: GAD Pelileo

Recuperado de: http://pelileo.gob.ec/html/images/lotaip2018/febrero/Literal_b1-Directorio_de_la_institucion.pdf

Se procedió a aplicar la fórmula matemática y se determina la muestra representativa para el desarrollo del presente trabajo de investigación.

$$n = \frac{Z^2NPQ}{Z^2PQ + (N-1)e^2}$$

En donde:

n= tamaño de la muestra

Z= nivel de confianza 95% (1,96)

P= probabilidad de ocurrencia 0,5

Q= probabilidad de no ocurrencia 1-0,5= 0,5

N= población (278)

e= error de muestreo 5% (0,05)

Aplicación de la fórmula:

$$n = \frac{1{,}96^2 * 278 * 0{,}5 * 0{,}5}{1{,}96^2 * 0{,}5 * 0{,}5 + (278 - 1) * 0{,}05^2}$$

$$n = \frac{266{,}9912}{0{,}09604 + 0{,}6925}$$

$$n = \frac{266{,}9912}{1{,}6529}$$

$$n = 161{,}53$$

$$n = 162$$

La muestra representativa para realizar el presente trabajo de investigación es de 162.

3.5. RESULTADOS

Resultados de la Encuesta aplicada al Jefe y Técnicos Profesionales de la Unidad de Gestión Tecnológica (UGT) del GAD Municipal del Cantón San Pedro de Pelileo.

1. **El acceso al lugar donde se ubica el área de sistemas está restringido para el personal no autorizado.**

Tabla N° 6: Acceso restringido al área de sistemas

Manifestación	N° de personas encuestadas	Porcentaje
Si	0	0%
No	3	100%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 6, el 100% de las personas encuestadas respondieron que el área de sistemas no se encuentra restringida para el acceso de personal no autorizado.

Gráfico N° 4: Acceso al área de sistemas

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N°4, en la encuesta aplicada al personal de la UGT, niega contar con un control de acceso al área de sistemas. Sin embargo el ingreso al centro de procesamiento de datos se encuentra restringido.

2. El área de sistemas cuenta con cámaras de seguridad internas y externas?

Tabla N° 7: Seguridad en el área de sistemas

Manifestación	N° de personas encuestadas	Porcentaje
Si	0	0%
No	3	100%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 7, el 100% de las personas encuestadas respondieron que el área de sistemas no cuenta con cámaras de seguridad internas y externas.

Gráfico N° 5: Seguridad del área de sistemas

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 5, el personal de la UGT confirma la inexistencia de cámaras de seguridad internas y externas, en el área de sistemas, exponiendo al área a robos.

3. **El Centro de Procesamiento de Datos dispone de aire de precisión para regular la temperatura?**

Tabla N° 8: Regulación de temperatura del CPD

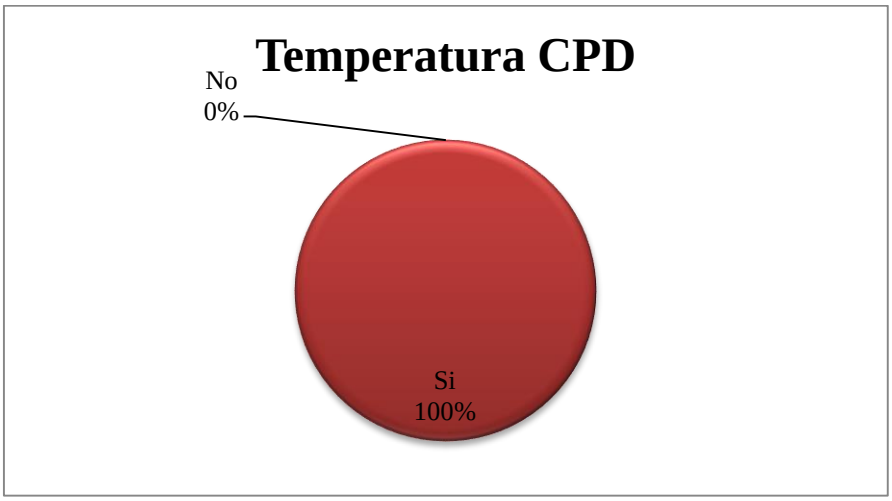
Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 8, el 100% de las personas encuestadas respondieron que el Centro de Procesamiento de Datos si cuenta con aires de precisión para regular la temperatura.

Gráfico N° 6: Temperatura de CPD



Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N°6, el personal de la UGT, afirma que el Centro de Procesamiento de Datos posee aires de precisión para regular la temperatura que garantice un buen funcionamiento de los servidores.

4. El lugar donde se ubica el área de sistemas cuenta con una salida de emergencia?

Tabla N° 9: Salida de emergencia para el área de sistemas

Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 9, el 100% de las personas encuestadas respondieron que el área de sistemas si cuenta con una salida de emergencia.

Gráfico N° 7: Salida de Emergencia

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 7, el personal de la UGT, afirma que el área de sistemas cuenta con una salida de emergencia, debidamente señalada, en caso de suscitarse alguna catástrofe.

5. El lugar donde se ubica el área de sistemas cuenta con sensores de humo?

Tabla N° 10: Sensores de humo

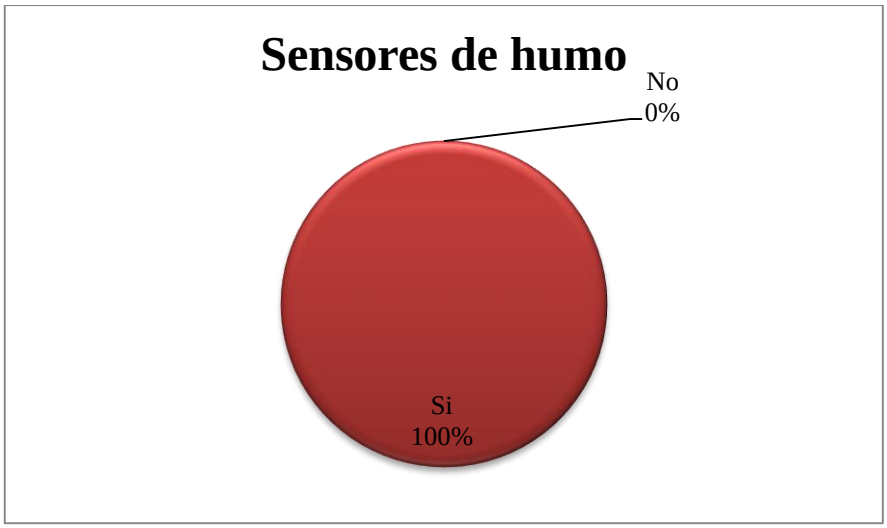
Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 10, el 100% de las personas encuestadas respondieron que el área de sistemas si cuenta con sensores de humo.

Gráfico N° 8: Sensores de humo



Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 8, el personal de la UGT, afirma que el área de sistemas cuenta con sensores de humo, los mismos que activarán la alerta para evacuación del edificio.

6. La señalética del área de sistemas es suficiente y se encuentra visible?

Tabla N° 11: Señalética suficiente

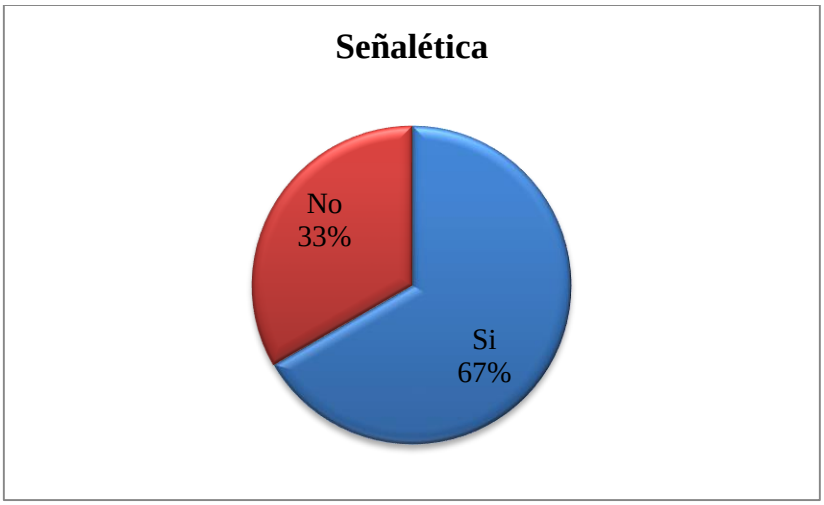
Manifestación	N° de personas encuestadas	Porcentaje
Si	2	67%
No	1	33%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 11, del 100% de las personas encuestadas, el 67% que corresponde a 2 personas afirma que el área de sistemas cuenta con la señalética suficiente y está visible, mientras que el 33% que corresponde a una persona respondió que el área de sistemas no posee la señalética suficiente.

Gráfico N° 9: Señalética



Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 9, el 67% de la totalidad de personas encuestadas, afirma la señalética existente es suficiente y se encuentra visible, mientras que el 33% señala que la señalética debe mejorar.

7. Los puntos del centro de datos están debidamente aterrizados (conexión a tierra)?

Tabla N° 12: Conexión a tierra

Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 12, el 100% de las personas encuestadas respondieron afirmativamente en cuanto a que la conexión a tierra está debidamente establecida para los puntos del centro de datos.

Gráfico N° 10: Conexión a tierra

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 10, el personal de la UGT, afirma que las conexiones a tierra se encuentran debidamente establecidas para evitar inconvenientes eléctricos y daño a los equipos informáticos de la institución.

8. Usted participa de los programas de capacitación institucionales?

Tabla N° 13: Capacitación al personal

Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 13, el 100% de las personas encuestadas respondieron que sí participan de los programas de capacitación institucionales.

Gráfico N° 11: Capacitación del personal

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 11, el personal de la UGT participa en los programas de capacitación que organiza la institución con el fin de mejorar sus competencias y actualizar sus conocimientos.

9. Las computadoras de la institución cuentan con una póliza de seguros?

Tabla N° 14: Póliza de seguros

Manifestación	N° de personas encuestadas	Porcentaje
Si	0	0%
No	3	100%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 14, el 100% de las personas encuestadas respondieron que las computadoras de la institución no cuentan con una póliza de seguros.

Gráfico N° 12: Póliza de Seguros

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 12, el personal de la UGT menciona que las computadoras de la institución no cuentan con una póliza de seguros, que proteja los equipos en caso de suscitarse alguna catástrofe.

10. La planificación para el área de sistemas se encuentra debidamente documentado?

Tabla N° 15: Documentación del área

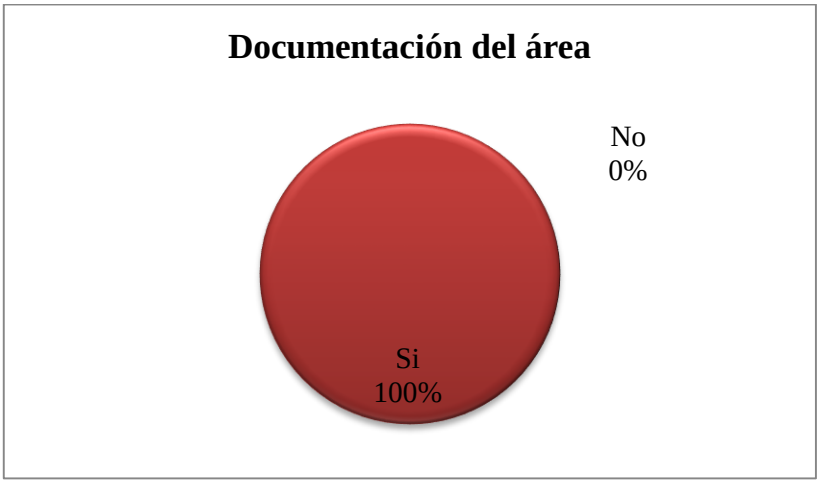
Manifestación	N° de personas encuestadas	Porcentaje
Si	3	100%
No	0	0%
Total	3	100%

Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 15, el 100% de las personas encuestadas respondieron afirmativamente en cuanto a que la planificación para el área de sistemas se encuentra debidamente documentados por escrito.

Gráfico N° 13: Documentación de la planificación



Fuente: Encuesta al personal de la UGT
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 13, el personal de la UGT afirma contar con la planificación debidamente documentada y aprobada por la máxima autoridad de la institución.

A continuación se puede apreciar los resultados de la encuesta aplicada a los servidores y servidoras del GAD Municipal del Cantón San Pedro de Pelileo, mediante la Escala de Likert que evalúa el nivel de satisfacción de los encuestados.

1. Usted cómo califica la atención que brinda el personal del área de sistemas:

Tabla N° 16: Atención que brinda el personal del área de sistemas

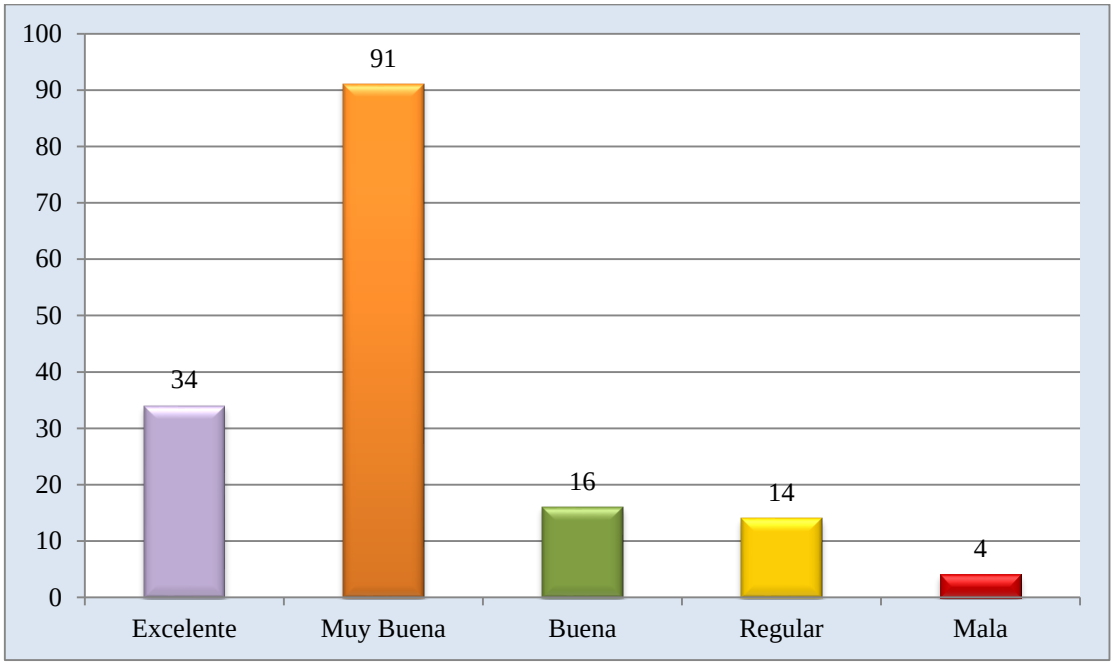
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	34	21%
Muy Buena	91	57%
Buena	16	10%
Regular	14	9%
Mala	4	3%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 16, del total de 159 personas encuestadas se determinó los siguientes resultados: 91 personas (57%) calificaron la atención que brinda el personal del área de sistemas como Muy Buena, 34 personas (21%) calificaron la atención como Excelente, 16 personas (10%) calificaron la atención como Buena, 14 personas (9%) calificaron como Regular y 4 personas (3%) calificaron como mala.

Gráfico N° 14: Atención del personal del área de sistemas



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 14, los servidores y servidoras del GAD Municipal del Cantón Pelileo calificaron como Muy Buena la atención que brinda el personal del área de sistemas, esto se debe a que el personal soluciona los inconvenientes que presenten los equipos informáticos para continuar con el normal desarrollo de las actividades.

2. **El sistema informático que utiliza para el desarrollo de sus actividades laborales es:**

Tabla N° 17: Calificación del Sistema

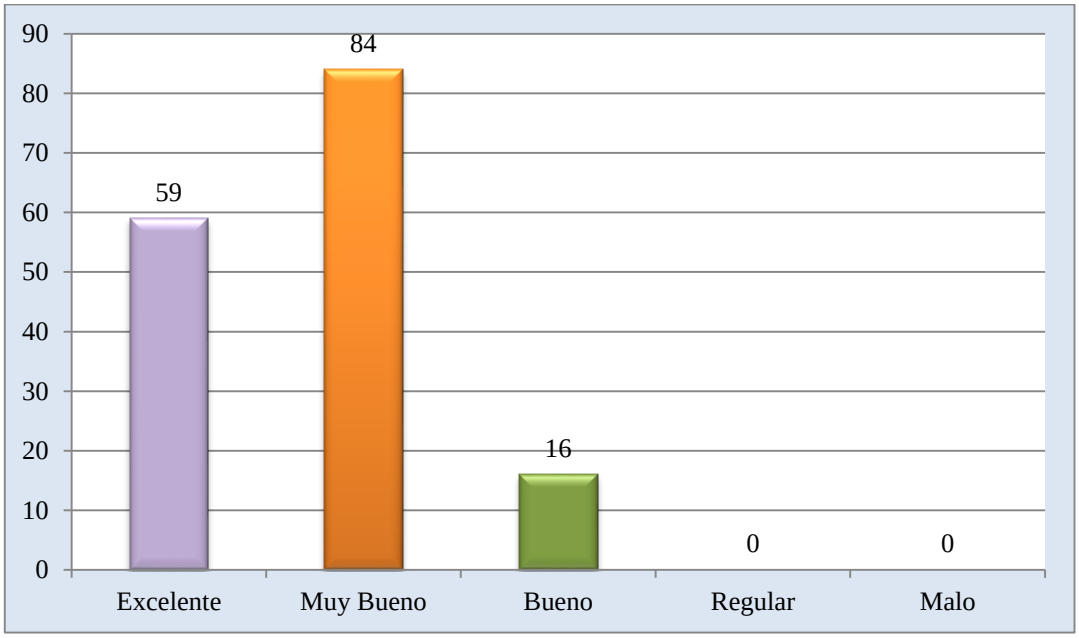
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	59	37%
Muy Bueno	84	53%
Bueno	16	10%
Regular	0	0%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar la tabla N° 17, del total de 159 personas encuestadas se determinó lo siguiente: 84 personas (53%) calificaron al sistema como Muy Bueno, mientras que 59 personas (37%) calificaron al sistema como Excelente, 16 personas (10%) calificaron el sistema como Bueno, no se registran datos en Regular y Malo.

Gráfico N° 15: Calificación del Sistema



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en gráfico N° 15, no se registran datos en la calificación de Regular y Malo, esto se debe a que el sistema con el que laboran los servidores públicos del GAD de Pelileo, presenta varios módulos que permite interacción entre los usuarios internos, por lo que la calificación que se destaca es de Muy Bueno.

3. **Considera que las políticas sobre el uso de los equipos informáticos en su lugar de trabajo son:**

Tabla N° 18: Políticas de uso de los equipos informáticos

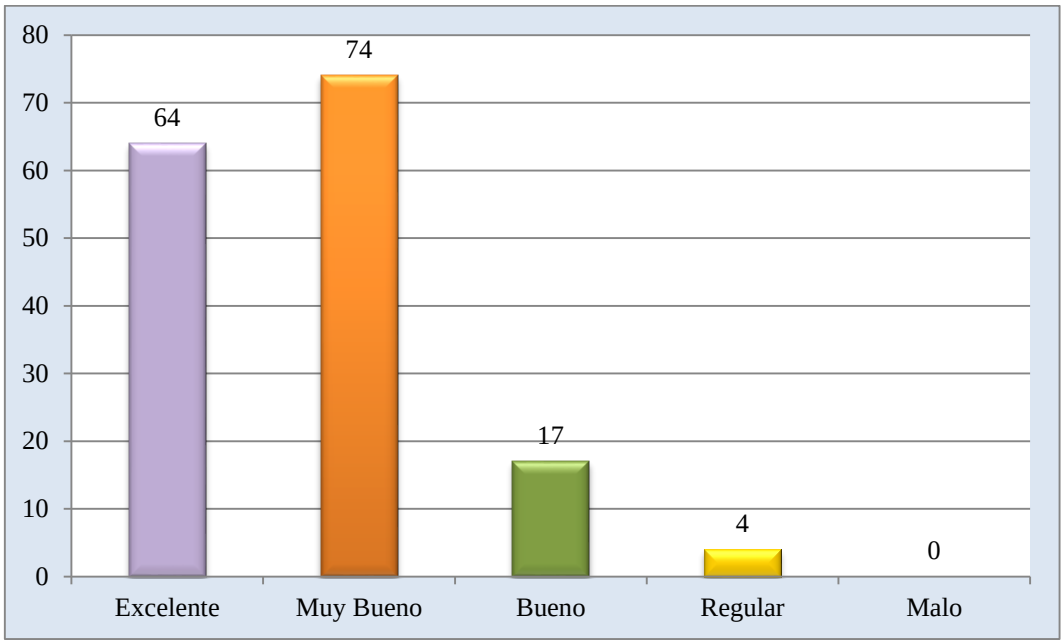
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	64	40%
Muy Bueno	74	47%
Bueno	17	11%
Regular	4	3%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 18, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 74 personas (47%) calificaron a las políticas como Muy Bueno, 64 personas (40%) como Excelente, 17 personas (11%) calificaron como Bueno, 4 personas (3%) calificaron como Regular.

Gráfico N° 16: Políticas de uso de los equipos informáticos



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 16, la calificación que se destaca es Muy Bueno, además se puede observar la calificación de Regular porque a pesar de que los instructivos se encuentran establecidos, los servidores no cumplen con las políticas sobre el uso de los equipos informáticos.

4. **Cómo califica el servicio de internet que brinda el GAD Municipal del Cantón San Pedro de Pelileo?**

Tabla N° 19: Servicio de Internet

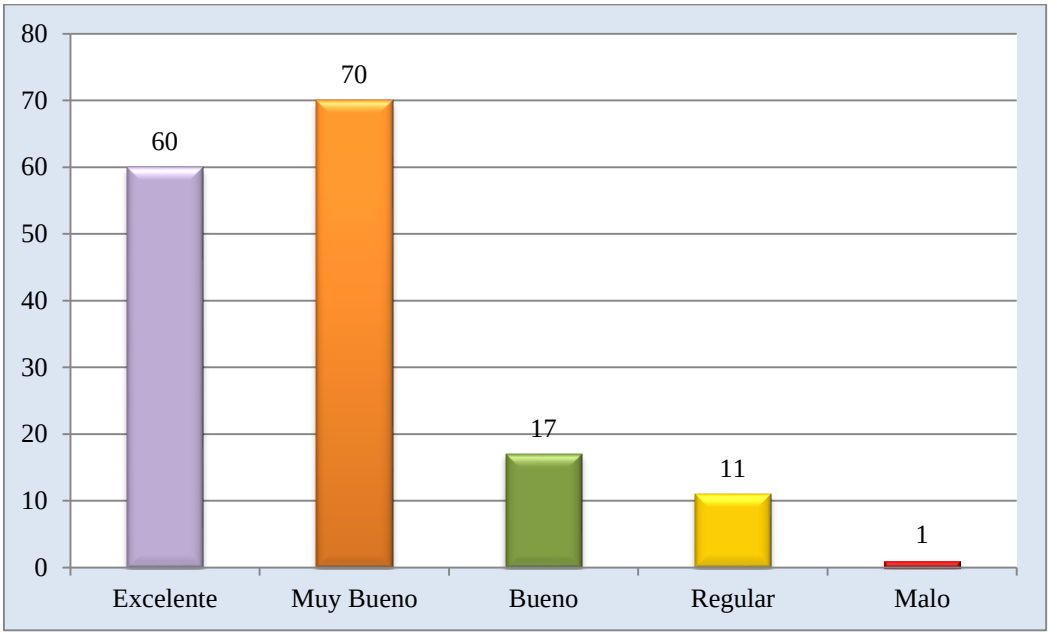
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	60	38%
Muy Bueno	70	44%
Bueno	17	11%
Regular	11	7%
Malo	1	1%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 19, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 70 personas (44%) considera que el servicio de internet es Muy Bueno, mientras que 60 personas (38%) califica este servicio como Excelente, 17 personas (11%) considera que el servicio de internet es Bueno, 11 personas (7%) califican el internet como Regular y finalmente 1 persona (1%) califican el internet como Malo.

Gráfico N° 17: Servicio de Internet



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 17, la mayoría de servidores calificaron el servicio de Internet como Muy Bueno, también se observa la calificación Regular, debido a que en ocasiones los servidores se han quedado sin internet para cumplir con las funciones asignadas.

5. **Considera que la utilización de claves fuertes para encender el computador es una medida de seguridad:**

Tabla N° 20: Claves de acceso para encender el computador

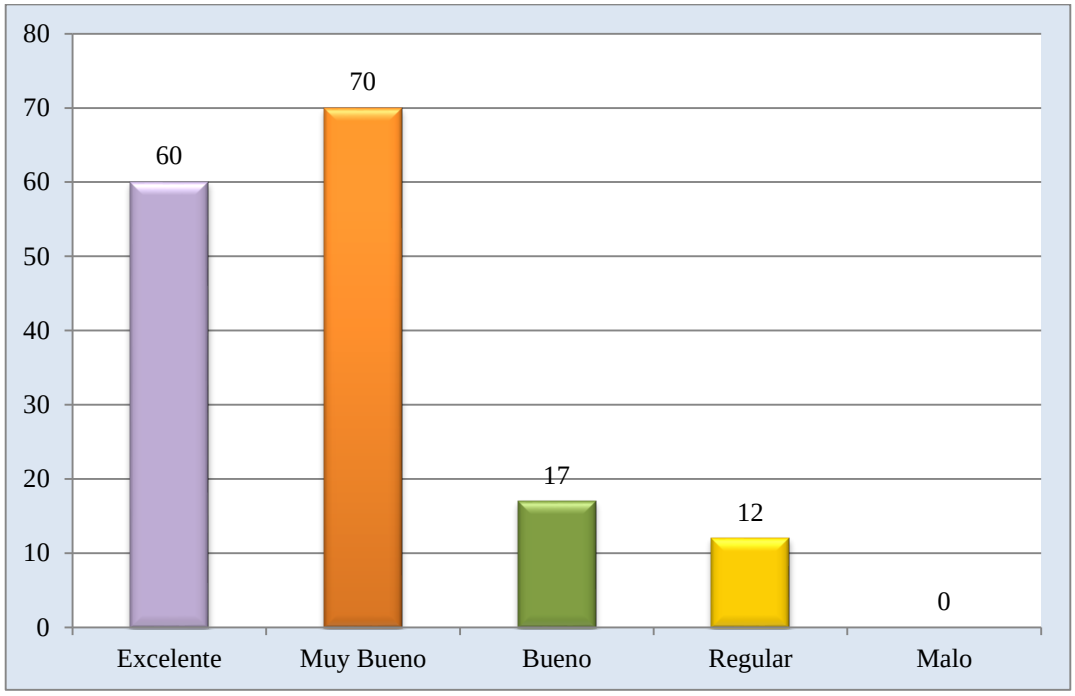
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	60	38%
Muy Bueno	70	44%
Bueno	17	11%
Regular	12	8%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 20, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 70 personas (44%) considera que el uso de claves fuertes para encender el computador es Muy Bueno, mientras que 60 personas (38%) calificaron como Excelente, 17 personas (11%) calificaron como Bueno, 12 personas (8%) calificaron como Regular y finalmente no se registró datos en la calificación Malo.

Gráfico N° 18: Claves de acceso para encender el computador



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 18, la mayoría de servidores calificaron el uso de claves fuertes para encender el computar como Muy Bueno seguido de una calificación Excelente, existe la calificación de regular debido a que el uso de claves fuertes para encender el computador toma tiempo para iniciar sus actividades laborales.

6. **Como califica la utilización de claves fuertes para ingresar al sistema informático Cabildo?**

Tabla N° 21: Claves de acceso para ingresar al sistema

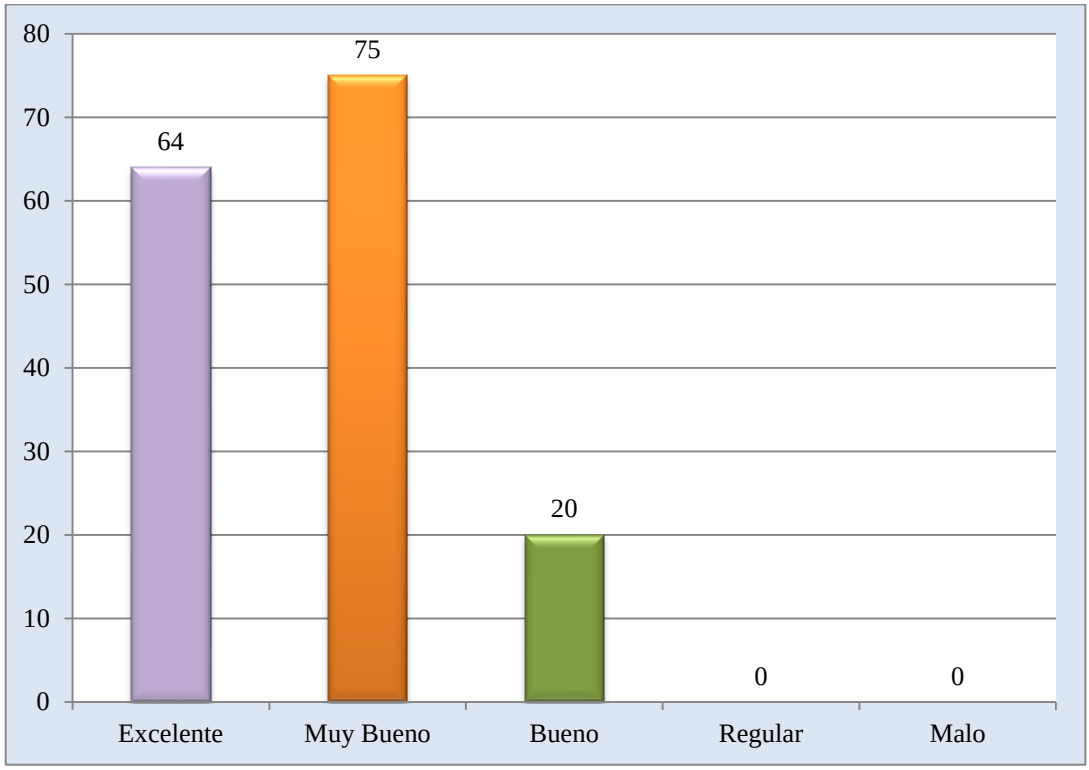
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	64	40%
Muy Bueno	75	47%
Bueno	20	13%
Regular	0	0%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 21, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 75 personas (47%) considera que el uso de claves fuertes para ingresar al sistema informático Cabildo es Muy Bueno, mientras que 64 personas (40%) calificaron como Excelente, 20 personas (13%) calificaron como Bueno, finalmente no se registraron datos en las calificaciones Regular y Malo.

Gráfico N° 19: Claves de acceso para ingresar al sistema



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 19, la mayoría de servidores calificaron el uso de claves fuertes para ingresar al sistema como Muy Bueno seguido de una calificación Excelente, además no se registran datos en calificaciones como Regular y Malo, debido a que el personal del área de sistemas, al ingresar un nuevo servidor o servidora pública, asigna un usuario y contraseña, la misma que es de completa responsabilidad del servidor/a.

7. Cada qué tiempo realiza la renovación de claves personales para uso del sistema?

Tabla N° 22: Frecuencia de renovación de claves

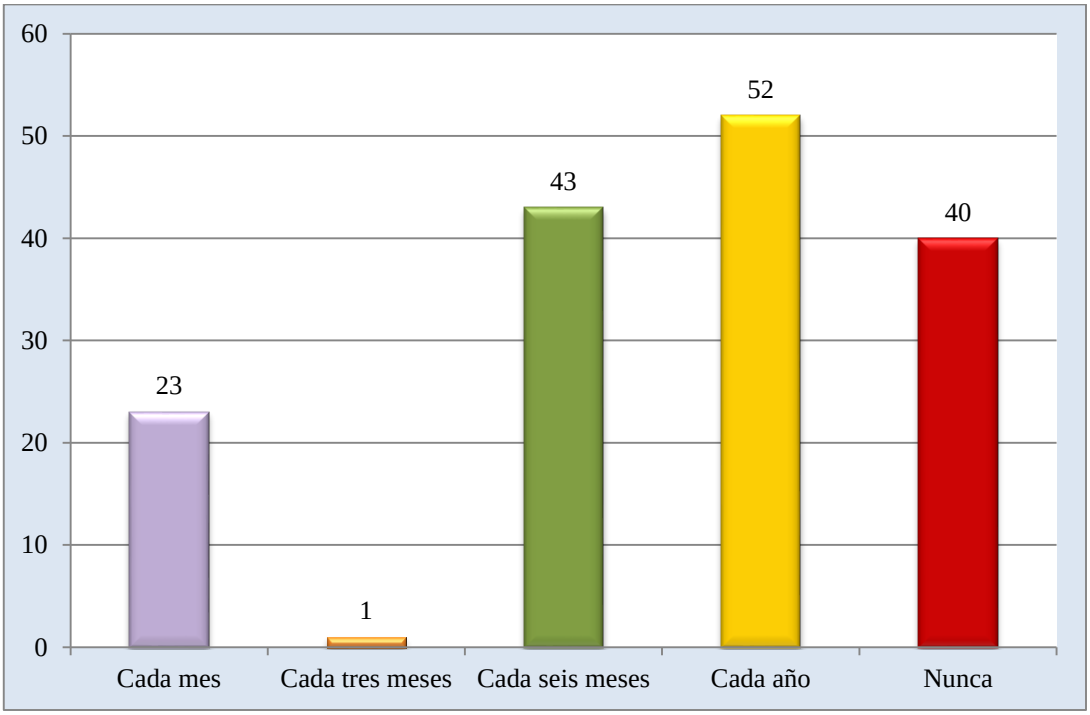
Manifestación	N° de personas encuestadas	Porcentaje
Cada mes	23	14%
Cada tres meses	1	1%
Cada seis meses	43	27%
Cada año	52	33%
Nunca	40	25%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 22, de 159 personas encuestadas se determinó los siguientes resultados con respecto a la frecuencia para renovación de claves: 52 personas (33%) realiza la realización de claves cada año, mientras que 43 personas (27%) cambia la clave cada seis meses, 40 personas (25%) Nunca ha cambiado su clave, 23 personas (14%) afirma cambiar la clave personal cada mes y 1 persona (1%) cambia su clave cada tres meses.

Gráfico N° 20: Frecuencia de renovación de claves



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 20, la frecuencia de renovación de claves con mayor aplicación es Cada año, además la encuesta revela que los servidores/as Nunca han cambiado su clave, aunque resulte tedioso, el cambio de clave es una medida de seguridad que los servidores y servidoras públicas deben conocer y aplicar con el fin de garantizar la integridad y confiabilidad de la información.

8. **Considera que la utilización de políticas institucionales para la renovación de claves personales es:**

Tabla N° 23: Uso política institucional para renovación de claves

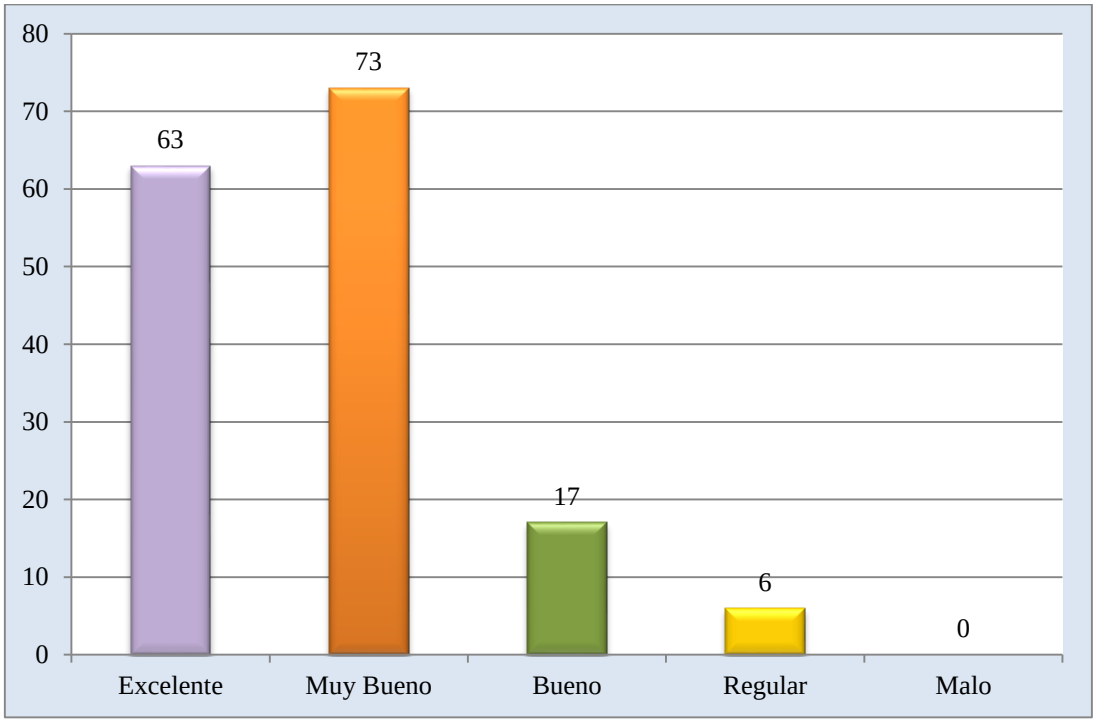
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	63	40%
Muy Bueno	73	46%
Bueno	17	11%
Regular	6	4%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 23, de 159 personas encuestadas se determinó los siguientes resultados con respecto al uso de políticas para la renovación de claves: 73 personas (46%) calificaron como Muy Bueno, mientras que 63 personas (40%) calificaron como Excelente, 17 personas (11%) calificaron como Bueno y finalmente 6 personas (4%) calificaron como Regular.

Gráfico N° 21: Uso de política institucional para renovación de claves personales



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 21, la mayoría de personas encuestadas calificaron el uso de políticas para renovación de claves personales como Muy Bueno, la correcta aplicación de los protocolos existentes puede salvaguardar la información.

9. **Considera que el plan de contingencias y medidas de seguridad ante riesgos que ocasionen daño a los equipos informáticos son:**

Tabla N° 24: Plan de contingencias y medidas de seguridad ante riesgos que puedan ocasionar daño a los equipos informáticos

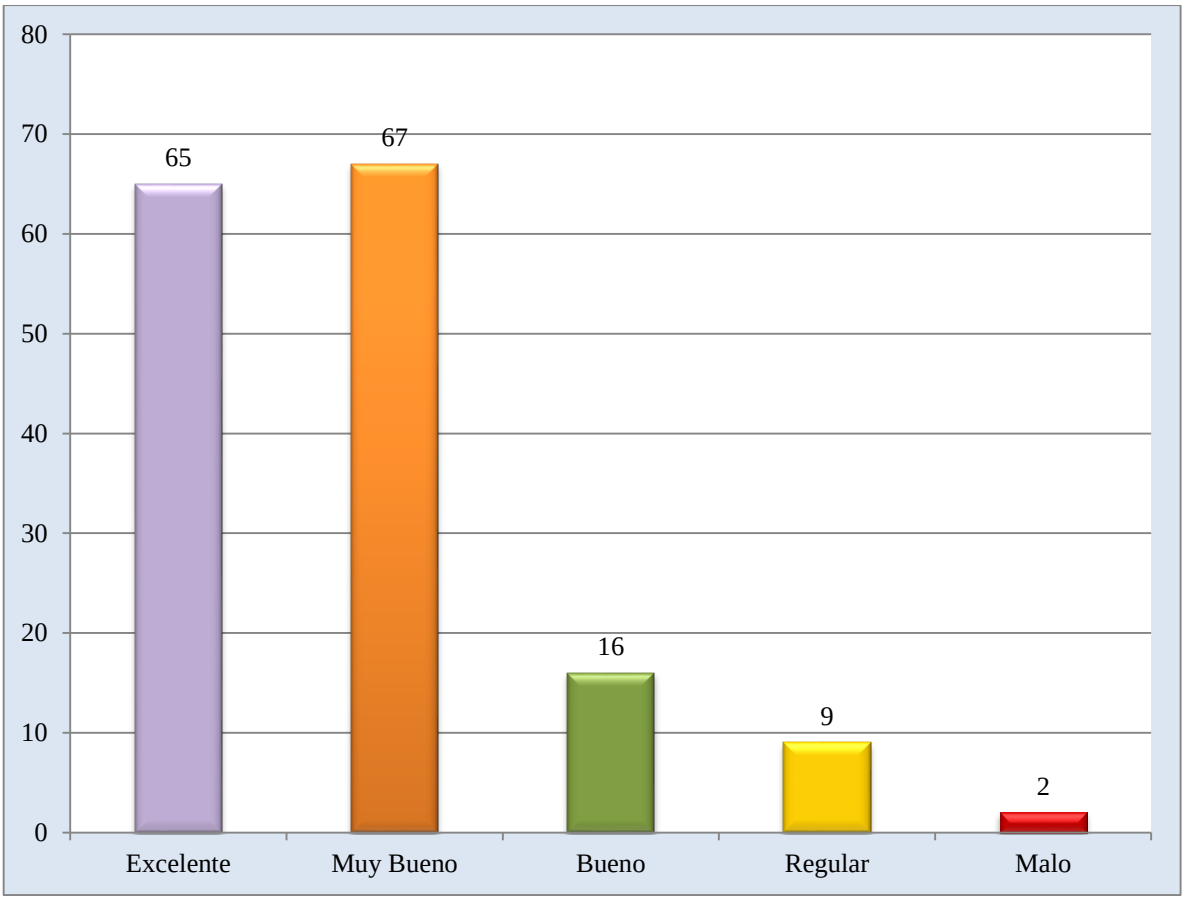
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	65	41%
Muy Bueno	67	42%
Bueno	16	10%
Regular	9	6%
Malo	2	1%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 24, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 67 personas (42%) calificaron el plan de contingencias y medidas de seguridad como Muy Bueno, mientras que 65 personas (41%) calificaron como Excelente, 16 personas (10%) calificaron como Bueno, 9 personas (6%) calificaron como regular y finalmente 2 personas (1%) calificaron como Malo.

Gráfico N° 22: Plan de contingencias y medidas de seguridad ante riesgos que ocasionen daño a los equipos informáticos



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 22, la mayoría de las personas encuestadas calificaron al plan de contingencias y medidas de seguridad ante riesgos que ocasionen daño a los equipos informáticos como Muy Bueno (67) y Excelente (65). Sin embargo existen registros de calificaciones como Regular y Malo lo que incide directamente en la seguridad física de los equipos informáticos de la institución.

10. Cómo califica su lugar de trabajo si cuenta con los equipos necesarios como UPS con regulador de voltaje que permita continuar en sus actividades en caso de corte de energía:

Tabla N° 25: Lugar de Trabajo Equipado

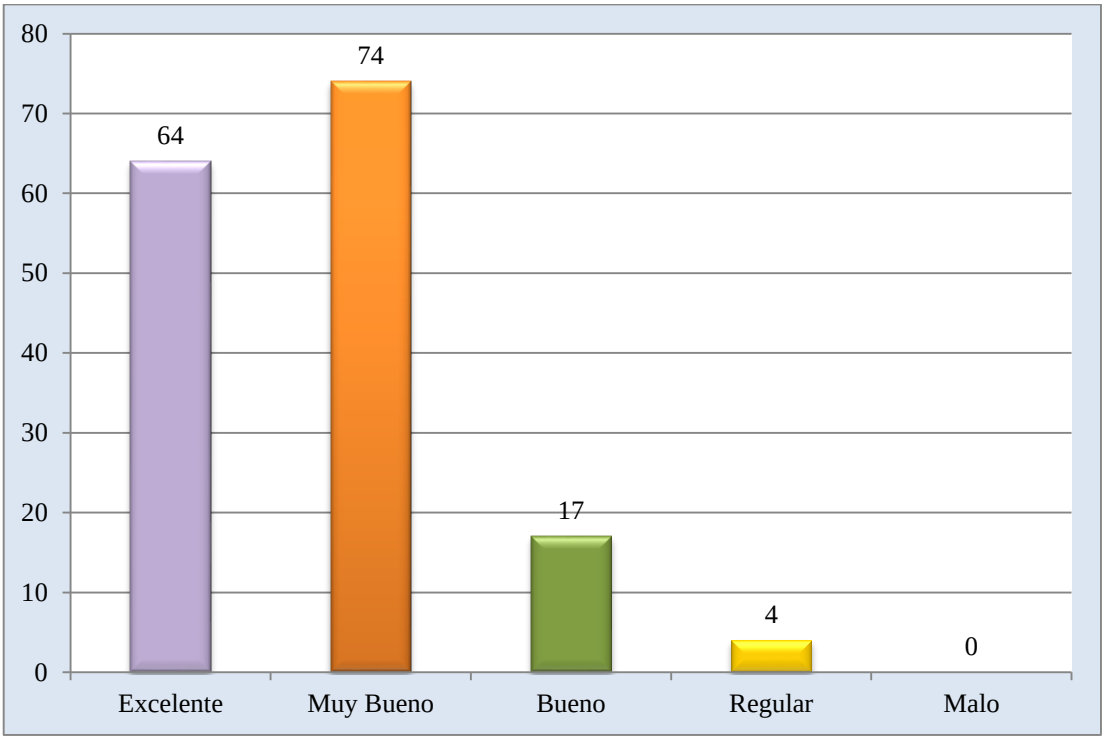
Manifestación	N° de personas encuestadas	Porcentaje
Excelente	64	40%
Muy Bueno	74	47%
Bueno	17	11%
Regular	4	3%
Malo	0	0%
Total	159	100%

Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Análisis:

Como se puede observar en la tabla N° 25, del total de 159 personas encuestadas se determinó los resultados que se detallan a continuación: 74 personas (47%) calificaron su lugar de trabajo como Muy Bueno, mientras que 64 personas (40%) calificaron como Excelente, 17 personas (11%) calificaron como Bueno, 4 personas (3%) calificaron como regular y finalmente no se registró datos en la calificación Malo.

Gráfico N° 23: Lugar de Trabajo equipado



Fuente: Encuesta aplicada a los servidores y servidoras del GADMCSPP
Elaboración: Autora

Interpretación:

Como se puede observar en el gráfico N° 23, la mayoría de personas encuestadas califica su lugar de trabajo como Muy Bueno debido a que si cuentan con equipos necesarios como UPS con regulador de voltaje que permita continuar en sus actividades en caso de corte de energía.

3.6. VERIFICACIÓN DE LA IDEA A DEFENDER

Una vez que se han obtenido y analizado los resultados se concluye que existe el incumplimiento de políticas internas, así como la falta de medidas que contribuyan a la seguridad informática, física y lógica de la institución, lo que afecta a la integridad, confiabilidad y disponibilidad de la información.

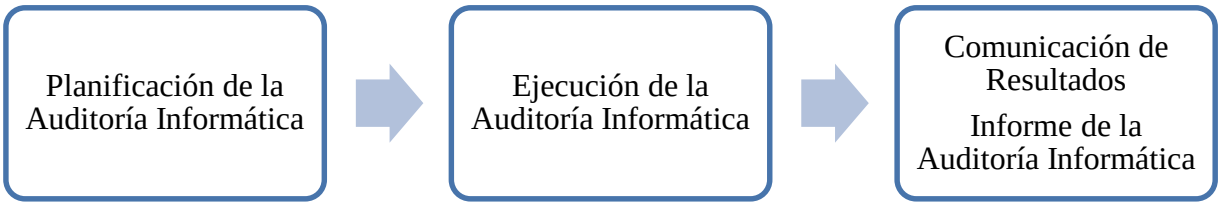
CAPÍTULO IV: MARCO PROPOSITIVO

4.1. AUDITORÍA INFORMÁTICA A LA UNIDAD DE GESTIÓN TECNOLÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO, PROVINCIA DE TUNGURAHUA, PERÍODO 2016.

4.2. CONTENIDO DE LA PROPUESTA

Para la realización del presente trabajo de investigación se presenta a continuación la metodología aplicando el COSO I para las entidades del sector público:

Gráfico N° 24: Metodología de la Auditoría Informática



Elaboración: Autora

4.2.1. Archivo Permanente

ARCHIVO PERMANENTE

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

Razón Social	**Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo**
RUC	1860000640001
Provincia	Tungurahua
Dirección	Avenida 22 de Julio S/N y Padre Chacón
Teléfono	03) 2871121 / 2871125 **Fax:** 03) 2871207
Correo Electrónico	municipiodepelileo@hotmail.com
Página Web	www.pelileo.gob.ec

Fuente: GAD Municipal de Pelileo
Elaboración: Autora

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

El Cantón Pelileo es una municipalidad de la Provincia de Tungurahua. Su cabecera cantonal es la ciudad de San Pedro de Pelileo.

Pelileo fue un pequeño pueblo fundado por el español Antonio Clavijo en el año de 1570 y mediante decreto expedido por el Gobierno Provisorio el 3 de Julio de 1860, se creó el Cantón Pelileo y elevó al estatus de Provincia a Tungurahua.

Mediante decreto particular dictado por el Jefe Civil y Militar, don Antonio Muñoz, con fecha 22 de julio de 1860, en el artículo 3 menciona que por primera vez y en razón de que no se estableció la orden municipal, el Jefe Superior otorgaría los nombramientos de Jefe Político, Alcalde Municipal, Concejeros, Procurador Síndico y más empleados del Cantón, los mismos que serían posesionados mediante juramento ante el Gobernador de la Provincia. Fue así como Pelileo inició sus actividades municipales el 31 de Julio de mismo año.

En el año de 1949, un día viernes 5 de agosto aproximadamente a las dos de la tarde se suscitó una catástrofe que destruyó a Pelileo, un terremoto de 7,8 grados en la escala de Richter, dio como resultado un sitio desolado, familias destruidas. En aquel entonces el Presidente de la República Galo Plaza Lasso conjuntamente con ayuda internacional destinaron recursos para su posterior reconstrucción.

Pelileo resurge de entre los escombros, sus hijos, hombres y mujeres emprendedoras con su arduo trabajo, como es la confección del jean, por esta razón se le conoce como la “ciudad azul”, se logra el desarrollo del nuevo Edén del Ecuador. Y años más tarde, el Presidente José María Velasco Ibarra, perdona la deuda a los pelileños por la adquisición de las casas que se les fueron otorgadas después del terremoto.

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

El Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo tiene las siguientes competencias de acuerdo a lo que establece la Constitución de la República del Ecuador (Art. 264):

1. Planificación del desarrollo cantonal y formulación de los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, provincial y parroquial, con el fin de regular el uso y la ocupación del suelo urbano y rural.

2. Ejercer el control sobre el uso y ocupación del suelo en el cantón.

3. Planificar, construir y mantener la vialidad urbana.

4. Prestar los servicios públicos de agua potable, alcantarillado, depuración de aguas residuales, manejo de desechos sólidos, actividades de saneamiento ambiental y aquellos que establezca la ley.

5. Crear, modificar o suprimir mediante ordenanzas, tasas y contribuciones especiales de mejoras.

6. Planificar, regular y controlar el tránsito y el transporte público dentro de su territorio cantonal.

7. Planificar, construir y mantener la infraestructura física y los equipamientos de los espacios públicos destinados al desarrollo social, cultural y deportivo de acuerdo con la ley.

Previa autorización del ente rector de la política pública podrán construir y mantener la infraestructura física y los equipamientos de salud y educación.

8. Preservar, mantener y difundir el patrimonio arquitectónico, cultural y natural del cantón y construir los espacios públicos para estos fines.

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

9. Formar y administrar los catastros inmobiliarios urbanos y rurales

10. Delimitar, regular, autorizar y controlar el uso de las playas de mar, riberas y lechos de ríos, lagos y lagunas, sin perjuicio de las limitaciones que establezca la ley.

11. Preservar y garantizar el acceso efectivo de las personas al uso de las playas de mar, riberas de ríos, lagos y lagunas.

12. Regular, autorizar y controlar la explotación de materiales áridos y pétreos, que se encuentren en los lechos de los ríos, lagos, playas de mar y canteras.

13. Gestionar los servicios de prevención, protección, socorro y extinción de incendios.

14. Gestionar la cooperación internacional para el cumplimiento de sus competencias.

Fines del GAD Municipal del Cantón San Pedro de Pelileo

a. El desarrollo equitativo y solidario mediante el fortalecimiento del proceso de autonomías y descentralización;

b. La garantía, sin discriminación alguna y en los términos previstos en la Constitución de la República, de la plena vigencia y el efectivo goce de los derechos individuales y colectivos constitucionales y de aquellos contemplados en los instrumentos internacionales;

c. El fortalecimiento de la unidad nacional en la diversidad;

d. La recuperación y conservación de la naturaleza y el mantenimiento de un ambiente sostenible y sustentable;

e. La protección y promoción de la diversidad cultural y el respeto a sus espacios de generación e intercambio; la recuperación, preservación y desarrollo de la memoria social y el patrimonio cultural;

f. La obtención de un hábitat seguro y saludable para los ciudadanos y la garantía de su derecho a la vivienda en el ámbito de sus respectivas competencias;

g. El desarrollo planificado participativamente para transformar la realidad y el impulso de la economía popular y solidaria con el propósito de erradicar la pobreza, distribuir equitativamente los recursos y la riqueza, y alcanzar el buen vivir;

h. La generación de condiciones que aseguren los derechos y principios reconocidos en la Constitución a través de la creación y funcionamiento de sistemas de protección integral de sus habitantes; y,

i. Los demás establecidos en la Constitución y la ley.

Políticas del GAD Municipal del Cantón San Pedro de Pelileo

a. Garantizar el uso eficiente de los recursos institucionales bajo principios de seguridad, eficiencia, sostenibilidad y responsabilidad en función de los estándares del ciudadano.
b. Asegurar la diversidad de funciones y de las operaciones institucionales; y, canalizar los recursos hacia la inversión y gasto social prioritario.
c. Propender a la universalización de las operaciones expandiendo la cobertura a todo el Cantón, procurando compatibilidad entre los fondos institucionales, las transferencias y la inversión con el servicio y obra pública.
d. Promover condiciones competitivas dentro de la dinámica productiva y comercial del Cantón.
e. Garantizar transparencia y eficiencia en la gestión del Gobierno Municipal, incorporando mecanismos de evaluación y rendición de cuentas, respetando la aplicación de normas, manuales y resoluciones.

f. Fomentar la observancia plena del COOTAD, LOSEP, Reglamentos Código de ética en los diferentes procesos y en la gestión del GADMSPP.

g. Instrumentar mecanismos que permitan mitigar el riesgo en las operaciones de inversión pública municipal.

h. Incorporar como parte de la cultura del Gobierno la administración integral de riesgos y la política de mejoramiento continuo de la calidad para el Buen Vivir.

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

GAD Municipal del Cantón San Pedro de Pelileo

Misión

Mejorar la calidad de vida de los habitantes del Cantón Pelileo, con una cuidadosa planificación, regulación y entrega de servicios e infraestructura pública.

Visión

Ser un gobierno participativo, ejemplo de trabajo e integridad, generador de oportunidades, y garante de derechos de los ciudadanos, del medio ambiente y del patrimonio cantonal.

Valores y Principios Institucionales

- Solidaridad
- Competitividad
- Honradez
- Responsabilidad social
- Justicia y equidad
- Respeto y pluralismo
- Protección al medio ambiente
- Eficiencia y eficacia
- Trabajo en equipo
- Participación ciudadana

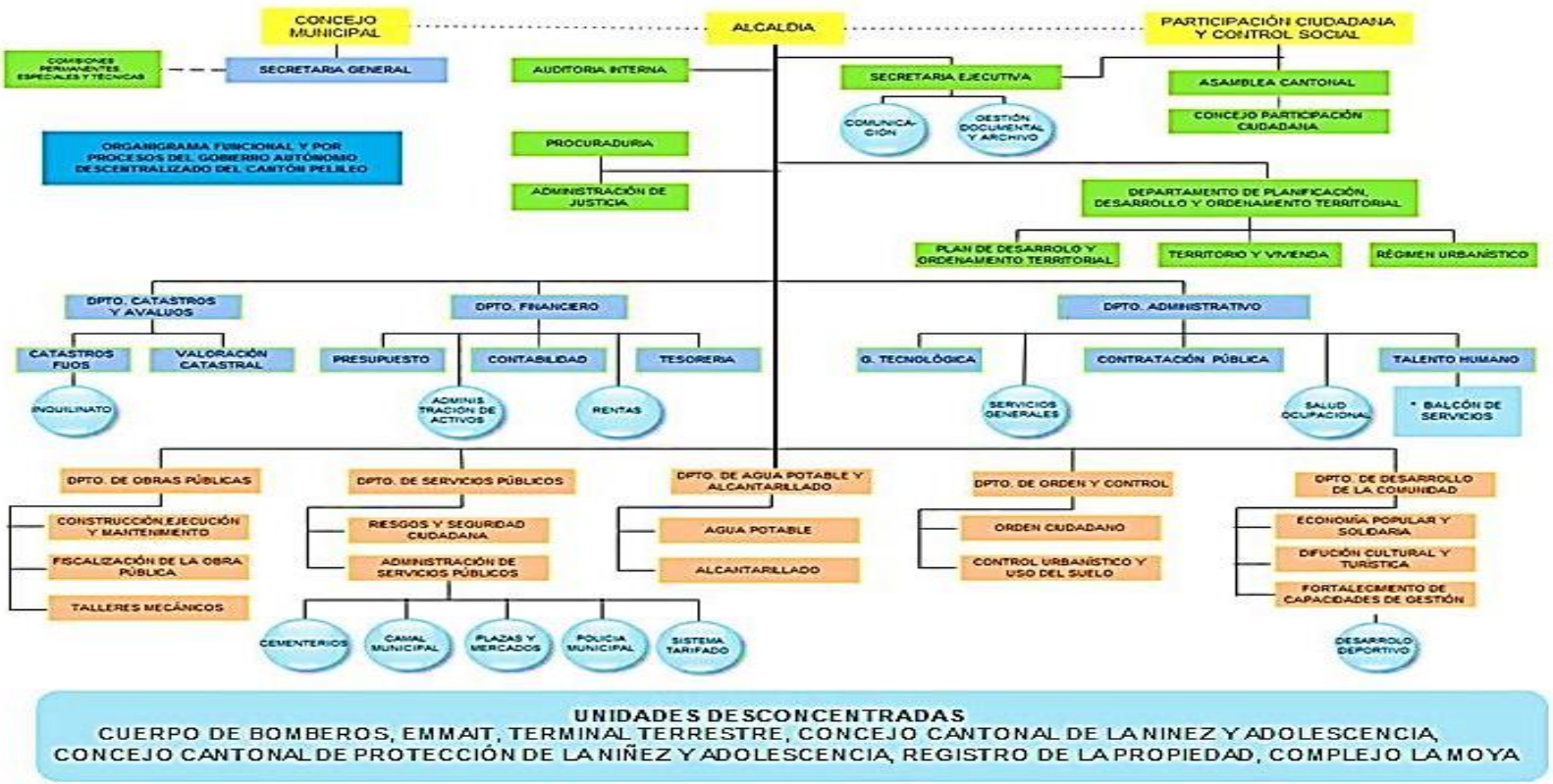
Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

La base legal que rige a la institución se puede apreciar a continuación:

- Constitución de la República del Ecuador
- Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD)
- Código de Trabajo
- Código de la Niñez y Adolescencia
- Ley Orgánica de la Función de Transparencia y Control Social
- Ley Orgánica del Servicio Público (LOSEP) y su Reglamento General (RGLOSEP)
- Ley Orgánica del Consejo de Participación Ciudadana y Control Social (CPCCS)
- Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su Reglamento General (RGLOSNCP)
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y su Reglamento
- Ley Orgánica de la Contraloría General del Estado y su Reglamento
- Normas Técnicas de Control Interno
- Estatuto Orgánico por Procesos institucional
- Reglamento de Talento Humano
- Reglamento de Seguridad y riesgos laborales

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

Estructura Organizacional del GAD Municipal del Cantón San Pedro de Pelileo



Recuperado de: www.pelileo.gob.ec

Elaborado Por:	JCVG	**Fecha:**	02-07-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	02-07-2018

Marca	Significado
*	Hallazgo
√	Revisado
∈	Verificación física
∞	Cotejado con evidencia

Elaborado Por:	JCVG	**Fecha:**	02-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	02-07-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	GAD Municipal del Cantón San Pedro de Pelileo Programa de Auditoría Del 1 de Enero al 31 de Diciembre del 2016	P/A 1/1

Objetivo General:

Establecer las formalidades con el cliente, mediante los diferentes documentos legales, para la aplicación de la Auditoría Informática.

Objetivos Específicos:

1. Realizar la fase contractual para llevar a cabo la Auditoría Informática.
2. Determinar los pasos a seguir en la aplicación de la Auditoría Informática.

N°	Procedimiento	Referencia P/T	Elaborado por	Fecha
1	Elabore el Programa de Auditoría	P/A 1/1	JCVG	03-07-2018
2	Realice la Carta de Presentación	C/P 1/1	JCVG	03-07-2018
3	Elabore la Propuesta de Trabajo para la Auditoría Informática	PR/T 1/4	JCVG	04-07-2018
4	Recepte la Carta de Aprobación de la Propuesta	C/A 1/1	JCVG	09-07-2018
5	Elabore el Contrato de Prestación de Servicios para la Auditoría Informática	C/PS 1/3	JCVG	10-07-2018
6	Emita la Orden de Trabajo	O/T 1/2	JCVG	11-07-2018
7	Notifique sobre el inicio del trabajo de Auditoría Informática	N/IA 1/1	JCVG	12-07-2018

Elaborado Por:	JCVG	**Fecha:**	03-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-07-2018

Riobamba, 03 de julio de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

Nos es grato poner a su consideración la propuesta de trabajo para la realización de una Auditoría Informática a la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo. Nuestro propósito es brindar servicios especializados fundamentados en conocimientos, creatividad, responsabilidad, transparencia y trabajo en equipo, que garantizan la entrega de un producto final que le permita tomar decisiones en beneficio de la institución.

Nuestro equipo de trabajo lo integran personas altamente competitivas, con experiencia y conocimientos informáticos, quienes están dirigidos por el supervisor de la firma auditora quien a la vez avala la calidad del trabajo.

A continuación ponemos a vuestra consideración la propuesta, la cual queda a su entera disposición. Por la favorable atención que se digne dar a la presente, anticipamos nuestro sincero agradecimiento.

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	03-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-07-2018

Riobamba, 04 de julio de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Estimado Doctor Manuel Caizabanda, nos es grato presentarle la propuesta de trabajo de servicios profesionales para llevar a cabo la Auditoría Informática a la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016.

Nuestra propuesta ha sido elaborada para cumplir con los requerimientos y demás disposiciones legales que regulan las actividades de la institución.

1. Objetivo General

Realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, para evaluar la seguridad de la información.

2. Objetivos Específicos

- Analizar los riesgos que inciden en la seguridad de la información de la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.
- Identificar los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

- Presentar el informe, al concluir el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

3. Alcance de la Auditoría Informática

El período que comprenderá la Auditoría Informática considera 1 de Enero al 31 de Diciembre del 2016.

4. Plazo

El plazo estimado para la realización de la Auditoría Informática es de 65 días laborables.

5. Honorarios

Cabe señalar que el desarrollo de la presente Auditoría Informática, tiene fines educativos, por lo que no se receptará ningún valor monetario.

6. Metodología del Trabajo

Para realizar la Auditoría Informática se aplicarán las Normas de Auditoría Generalmente Aceptadas y las Normas Técnicas de Control Interno establecidas por la Contraloría General del Estado

Elaborado Por:	JCVG	**Fecha:**	04-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	04-07-2018

7. Recursos Humanos

El Equipo de trabajo que integran la Firma Auditora "Fénix JVG Auditores & Consultores Asociados" constan las siguientes personas:

Nombres	Cargo
Ing. Willian Yanza	Supervisor
Dr. Carlos Buenaño	Jefe de Equipo
Johanna Villena	Auditora

8. Recursos Materiales

Cantidad	Detalle
7	Esferos azules
2	Esferos rojos
2	Lápices bicolores
1	Borrador
1	Sacapunta
1	Archivador
1	Resma de papel bond

9. Recursos Tecnológicos

Cantidad	Detalle
2	Computadores portátiles
1	Calculadora
1	Escáner
1	Cámara digital

Elaborado Por:	JCVG	**Fecha:**	04-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	04-07-2018

10. Cronograma de Actividades

Actividad	Días Estimados
Planificación	17
Ejecución	36
Informe	12
Total	65

Por la atención a la presente, extendemos nuestros más sinceros agradecimientos.

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	04-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	04-07-2018

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO
Alcaldía
Telf. 03 2871121/ 2871125 Ext. 106 FAX. (03) 2871207

Señor Ingeniero

Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

De mi consideración:

Reciba un afectuoso saludo a nombre del GADM-PELILEO y en el mío propio, por medio del presente me permito indicar que, después de analizar la propuesta de trabajo presentada, ha sido aceptada por la Municipalidad para su ejecución.

Esperando que el trabajo sea realizado según lo establecido me despido, augurándole éxitos en sus funciones.

Atentamente,

Dr. Manuel Caizabanda

ALCALDE DEL CANTÓN SAN PEDRO DE PELILEO

Av. 22 de Julio y Padre Chacón
www.pelileo.gob.ec
Pelileo – Tungurahua - Ecuador

Elaborado Por:	JCVG	**Fecha:**	09-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	09-07-2018

CONTRATO DE PRESTACIÓN DE SERVICIOS

En la ciudad de Riobamba a los diez días del mes de julio del año 2018, Provincia de Chimborazo, se celebra el presente contrato entre el Señor Dr. Manuel Caizabanda, en carácter de Alcalde del GAD Municipal del Cantón San Pedro de Pelileo, que a partir de ahora se denominará "Contratante" y por otra parte el Señor Ing. Willian Yanza, representante de la Firma Auditora FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS, en adelante "Auditor", quienes convienen celebrar un Contrato Civil de Prestación de Servicios Profesionales del tenor siguiente:

PRIMERA.- ANTECEDENTES

De conformidad con las necesidades presentes del GAD Municipal del Cantón San Pedro de Pelileo se ha resuelto contratar los servicios de una Auditoría Informática para evaluar la seguridad de la información en el período 2016.

SEGUNDA.- OBJETO DEL CONTRATO

El objeto del presente contrato es la realización de la Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, para evaluar la seguridad de la información. Al finalizar se entregará un informe elaborado de acuerdo a las Normas de Auditoría Generalmente Aceptadas y las Normas Técnicas de Control Interno.

TERCERA.- PLAZO

El plazo estimado es de 65 días laborables, contados a partir de la fecha en que se firme dicho contrato. El plazo fijado será prorrogado por causas no imputables al contratista, por falta de entrega oportuna de materiales e información o casos fortuitos debidamente comprobados.

CUARTA.- HONORARIOS

No existe valor establecido debido a que la realización de la Auditoría Informática tiene fines educativos.

QUINTA.- OBLIGACIONES DEL CONTRATANTE

El "contratante" se compromete a entregar oportunamente la información que el "auditor" requiera para que pueda llevar a cabo el trabajo de campo.

SEXTA.- OBLIGACIONES DEL AUDITOR

El "auditor" se compromete a entregar el informe final y comunicar los resultados, así como emitir recomendaciones para la toma de decisiones.

SEPTIMA.- DOMICILIO

Las partes de común acuerdo convienen en fijar los siguientes domicilios:

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

REPRESENTANTE: Ing. Willian Yanza

DIRECCIÓN: Panamericana Sur Km 1 $^{1}/_{2}$ Riobamba - Ecuador

TELÉFONO: 0979712825

GOBIERNO AUTONÓMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

REPRESENTANTE: Dr. Manuel Caizabanda

DIRECCIÓN: Av. 22 de Julio y Padre Jorge Chacón Pelileo – Ecuador

TELÉFONO: (03) 2871121/ 2871125 Ext. 106 Fax: (03) 2871207

Elaborado Por:	JCVG	**Fecha:**	10-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	10-07-2018

OCTAVA.- ACEPTACIÓN

Las partes declaran estar de acuerdo con el contenido de todas y cada una de las cláusulas del presente contrato, para lo cual lo suscriben con su firma y rúbrica en el mismo lugar y fecha ya indicados.

Ing. Willian Yanza
SUPERVISOR FIRMA AUDITORA FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Dr. Manuel Caizabanda
ALCALDE GAD MUNICIPAL DEL CANTÓN PELILEO

Elaborado Por:	JCVG	**Fecha:**	10-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	10-07-2018

ORDEN DE TRABAJO N° 001- FJVG-2018

Riobamba, 11 de julio de 2018

Estimados integrantes del Equipo Auditor

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Presente

De acuerdo al contrato realizado con el GAD Municipal del Cantón San Pedro de Pelileo, para la realización de una Auditoría Informática, informo se inicie con dicha Auditoría por el período comprendido entre el 1 de enero y 31 de diciembre de 2016. Se considera lo siguiente:

Objetivo General

Realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, para evaluar la seguridad de la información.

Objetivos Específicos

- Analizar los riesgos que inciden en la seguridad de la información de la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.
- Identificar los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

Elaborado Por:	JCVG	**Fecha:**	11-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	11-07-2018

- Presentar el informe, al concluir el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

Alcance de la Auditoría Informática

El período que comprenderá la Auditoría Informática considera 1 de Enero al 31 de Diciembre del 2016.

Plazo

El plazo estimado para la realización de la Auditoría Informática es de 65 días laborables.

Recurso Humano

Nombres	Cargo
Ing. Willian Yanza	Supervisor
Dr. Carlos Buenaño	Jefe de Equipo
Johanna Villena	Auditora

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	11-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	11-07-2018

OFICIO N° 001- - FJVG-2018

Riobamba, 12 de julio de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

De nuestra consideración:

El motivo del presente es para comunicar el inicio de la Auditoría Informática que será realizado conforme a las Normas Técnicas de Control Interno emitidas por la Contraloría General del Estado con respecto a la Norma 410 sobre Tecnologías de la Información y Comunicación, a fin de entregar un informe que contenga los hallazgos y recomendaciones que serán de utilidad para la toma de decisiones.

Además solicito de la manera más comedida la colaboración y facilidades por parte de los servidores y servidoras públicas, para recabar información pertinente que contribuyan al desarrollo de la Auditoría Informática.

Hacemos propicia la oportunidad para reiterarle nuestros más sinceros agradecimientos.

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	12-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	12-07-2018

4.2.2. Archivo Corriente

ARCHIVO CORRIENTE

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

Razón Social	**Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo**
RUC	1860000640001
Provincia	Tungurahua
Dirección	Avenida 22 de Julio S/N y Padre Chacón
Teléfono	03) 2871121 / 2871125 **Fax:** 03) 2871207
Correo Electrónico	municipiodepelileo@hotmail.com
Página Web	www.pelileo.gob.ec

Fuente: GAD Municipal de Pelileo

Elaboración: Autora

Elaborado Por:	JCVG	**Fecha:**	13-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	13-07-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **Índice de Archivo Corriente** **Del 1 de Enero al 31 de Diciembre del 2016**	**I/AC** **1/1**

ÍNDICE	**REF. P/T**
Archivo Corriente	**A/C 1/1**
Índice de Archivo Corriente	**I/AC 1/1**
FASE I: PLANIFICACIÓN DE LA AUDITORÍA INFORMÁTICA	
Programa de Auditoría Informática - **Planificación Preliminar** - **Planificación Específica**	**PAI/PA 1/1**
FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA	
Programa de Auditoría Informática - **Análisis Situacional** - **Cuestionarios**	**EAI/PA 1/1**
FASE III: COMUNICACIÓN DE RESULTADOS	
Programa de Auditoría Informática - **Elaboración del Informe**	**CR/PA 1/1**

Elaborado Por:	JCVG	**Fecha:**	13-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	13-07-2018

Objetivo General:

Obtener una visión general del ambiente de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo, mediante la observación y entrevista el Jefe de dicha unidad.

Objetivos Específicos:

1. Observar las instalaciones de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo.
2. Entrevistar al Jefe de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo.

N°	Procedimiento	Referencia P/T	Elaborado por	Fecha
1	Elabore el Programa de Auditoría	P/A 1/1	JCVG	16-07-2018
2	Elabore el informe de visita preliminar a la Unidad de Gestión Tecnológica	V/P 1/9	JCVG	17-07-2018
3	Realice la entrevista al Jefe de la Unidad de Gestión Tecnológica	E/JUGT 1/2	JCVG	18-07-2018
4	Elabore el Memorándum de Planificación	M/P 1/3	JCVG	19-07-2018
5	Realice la Carta de Requerimiento de Información	CRI 1/2	JCVG	24-07-2018

Elaborado Por:	JCVG	**Fecha:**	16-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	16-07-2018

4.2.2.1. Planificación Preliminar

VISITA PRELIMINAR

Fecha de Inicio: 17-07-2018 **Hora de Inicio:** 10:00

Fecha de Término: 17-07-2018 **Hora de Término:** 15:00

DATOS DE LA INSTITUCIÓN

Nombre de la Entidad: GAD Municipal del Cantón San Pedro de Pelileo

Dirección: Avenida 22 de Julio S/N y Padre Chacón

Ubicación: Pelileo – Tungurahua

Correo Electrónico: municipiodepelileo@hotmail.com

Teléfono: 03) 2871121 / 2871125 **Fax:** 03) 2871207

Horario de Trabajo: 08:00 a 17:00

BASE LEGAL DE CREACIÓN Y FUNCIONAMIENTO

- Constitución de la República del Ecuador
- Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD)
- Código de Trabajo
- Código de la Niñez y Adolescencia
- Ley Orgánica de la Función de Transparencia y Control Social
- Ley Orgánica del Servicio Público (LOSEP) y su Reglamento General (RGLOSEP)
- Ley Orgánica del Consejo de Participación Ciudadana y Control Social (CPCCS)
- Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su Reglamento General (RGLOSNCP)
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y su Reglamento
- Ley Orgánica de la Contraloría General del Estado y su Reglamento

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

- Normas Técnicas de Control Interno
- Estatuto Orgánico por Procesos institucional
- Reglamento de Talento Humano
- Reglamento de Seguridad y riesgos laborales

INFORMACIÓN GENERAL

MISIÓN

Mejorar la calidad de vida de los habitantes del Cantón Pelileo, con una cuidadosa planificación, regulación y entrega de servicios e infraestructura pública.

VISIÓN

Ser un gobierno participativo, ejemplo de trabajo e integridad, generador de oportunidades, y garante de derechos de los ciudadanos, del medio ambiente y del patrimonio cantonal.

POLÍTICAS

a. Garantizar el uso eficiente de los recursos institucionales bajo principios de seguridad, eficiencia, sostenibilidad y responsabilidad en función de los estándares del ciudadano.
b. Asegurar la diversidad de funciones y de las operaciones institucionales; y, canalizar los recursos hacia la inversión y gasto social prioritario.
c. Propender a la universalización de las operaciones expandiendo la cobertura a todo el Cantón, procurando compatibilidad entre los fondos institucionales, las transferencias y la inversión con el servicio y obra pública.
d. Promover condiciones competitivas dentro de la dinámica productiva y comercial del Cantón.

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

e. Garantizar transparencia y eficiencia en la gestión del Gobierno Municipal, incorporando mecanismos de evaluación y rendición de cuentas, respetando la aplicación de normas, manuales y resoluciones.

f. Fomentar la observancia plena del COOTAD, LOSEP, Reglamentos Código de ética en los diferentes procesos y en la gestión del GADMSPP.

g. Instrumentar mecanismos que permitan mitigar el riesgo en las operaciones de inversión pública municipal.

h. Incorporar como parte de la cultura del Gobierno la administración integral de riesgos y la política de mejoramiento continuo de la calidad para el Buen Vivir.

ACTIVIDAD PRINCIPAL

Actividades realizadas por municipios, prestación de servicios en beneficio de la población.

FUNCIONES

a) Promover el desarrollo sustentable de su circunscripción territorial cantonal, para garantizar la realización del buen vivir a través de la implementación de políticas públicas cantonales, en el marco de sus competencias constitucionales y legales;

b) Diseñar e implementar políticas de promoción y construcción de equidad e inclusión en su territorio, en el marco de sus competencias constitucionales y legales;

c) Establecer el régimen de uso del suelo y urbanístico, para lo cual determinará las condiciones de urbanización, parcelación, lotización, división o cualquier otra forma de fraccionamiento de conformidad con la planificación cantonal, asegurando porcentajes para zonas verdes y áreas comunales;

d) Implementar un sistema de participación ciudadana para el ejercicio de los derechos y la gestión democrática de la acción municipal;

e) Elaborar y ejecutar el plan cantonal de desarrollo, el de ordenamiento territorial y las políticas públicas en el ámbito de sus competencias y en su circunscripción territorial, de manera coordinada con la planificación nacional, regional, provincial y parroquial, y realizar en forma permanente, el seguimiento y rendición de cuentas sobre el cumplimiento de las metas establecidas;

f) Ejecutar las competencias exclusivas y concurrentes reconocidas por la Constitución y la ley y en dicho marco, prestar los servicios públicos y construir la obra pública cantonal correspondiente, con criterios de calidad, eficacia y eficiencia, observando los principios de universalidad, accesibilidad, regularidad, continuidad, solidaridad, interculturalidad, subsidiariedad, participación y equidad;

g) Regular, controlar y promover el desarrollo de la actividad turística cantonal, en coordinación con los demás gobiernos autónomos descentralizados, promoviendo especialmente la creación y funcionamiento de organizaciones asociativas y empresas comunitarias de turismo;

h) Promover los procesos de desarrollo económico local en su jurisdicción, poniendo una atención especial en el sector de la economía social y solidaria, para lo cual coordinará con los otros niveles de gobierno;

i) Implementar el derecho al hábitat y a la vivienda y desarrollar planes y programas de vivienda de interés social en el territorio cantonal;

j) Implementar los sistemas de protección integral del cantón que aseguren el ejercicio, garantía y exigibilidad de los derechos consagrados en la Constitución y en los instrumentos internacionales, lo cual incluirá la conformación de los consejos cantonales, juntas cantonales y redes de protección de derechos de los grupos de atención prioritaria. Para la atención en las zonas rurales coordinará con los gobiernos autónomos parroquiales y provinciales;

k) Regular, prevenir y controlar la contaminación ambiental en el territorio cantonal de manera articulada con las políticas ambientales nacionales;

l) Prestar servicios que satisfagan necesidades colectivas respecto de los que no exista una explícita reserva legal a favor de otros niveles de gobierno, así como la elaboración, manejo y expendio de víveres; servicios de faenamiento, plazas de mercado y cementerios;

m) Regular y controlar el uso del espacio público cantonal y, de manera particular, el ejercicio de todo tipo de actividad que se desarrolle en él, la colocación de publicidad, redes o señalización;

n) Crear y coordinar los consejos de seguridad ciudadana municipal, con la participación de la Policía Nacional, la comunidad y otros organismos relacionados con la materia de seguridad, los cuales formularán y ejecutarán políticas locales, planes y evaluación de resultados sobre prevención, protección, seguridad y convivencia ciudadana;

o) Regular y controlar las construcciones en la circunscripción cantonal, con especial atención a las normas de control y prevención de riesgos y desastres;

p) Regular, fomentar, autorizar y controlar el ejercicio de actividades económicas, empresariales o profesionales, que se desarrollen en locales ubicados en la circunscripción territorial cantonal con el objeto de precautelar los derechos de la colectividad;

q) Promover y patrocinar las culturas, las artes, actividades deportivas y recreativas en beneficio de la colectividad del cantón;

r) Crear las condiciones materiales para la aplicación de políticas integrales y participativas en torno a la regulación del manejo responsable de la fauna urbana; y,

s) Las demás establecidas en la ley.

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

DEFINICIÓN ORGÁNICA DE LAS FUNCIONES DEL GADMCSPP

El Gobierno Municipal plantea en la estructura orgánica las siguientes competencias y funciones:

Función Legislativa y de Fiscalización._ Tiene como función legislar y fiscalizar la gestión de la institución, esta facultad la ejerce el Concejo Municipal y directorios de empresas o mancomunidades de instituciones adscritas.

Función Ejecutiva._ Tiene como función representar legalmente, así como la dirección y control está a cargo del Alcalde.

- **Nivel Administrativo y Operativo._** Se encargan de asesorar, apoyar, producir y entregar productos/servicios, son responsables los diferentes directores departamentales, técnicos departamentales y jefes de sección.
- **Nivel Asesor y/o de Apoyo.-** Se encargan de brindar asesoría al GADMCSPP así como a los niveles jerárquicos, es responsable directo el Procurador Síndico.

Función de Participación Ciudadana y Control Social._ Tiene como función apoyar, intervenir y controlar en la gestión del GADMCSPP, están a cargo los ciudadanos legalmente calificados.

PROCESOS DEL GADMCSPP

Se estableció una serie de procesos para el cumplimiento de las actividades a cargo de las funciones antes vistas.

a) **Procesos Gobernantes._** Generan y emiten políticas, directrices, líneas de acción, normas, planes e instrumentos que dirigen la gestión del GADMCSPP.

b) **Procesos Habilitantes y/o de soporte._** Brindan asesoramiento y apoyo al proceso gobernante, orientan y dinamizan procesos y valoran los resultados.

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

c) **Procesos Agregadores de Valor._** Generan y facilitan productos/servicios orientados a la satisfacción de los ciudadanos, orientan a la misión, visión, competencias, funciones del GADMCSPP.

d) **Procesos Desconcentrados._** Representan la dirección compartida y trabajo en equipo. Son designados por la función ejecutiva del GADMCSPP, con el fin de asegurar la entrega de productos/servicios de calidad.

e) **Procesos Descentralizados._** Representan el trabajo en equipo, debido a la cesión de competencias y atribuciones con los respectivos recursos humanos y financieros, materiales y tecnológicos, del GADMCSPP hacia empresas públicas o mancomunidades.

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

FUNCIONARIOS PRINCIPALES

CARGO	NOMBRES
Alcalde	Dr. Manuel Caizabanda
Concejal Cantonal	Lcdo. José Aladino Carrasco
Concejal Cantonal	Ab. Martha Chango
Concejal Cantonal	Ab. Carmen Jerez
Concejal Cantonal	Ab. Freddy Leguízamo
Concejal Cantonal	Ab. María Augusta Llerena
Concejal Cantonal	Lcdo. Danilo Morales
Concejal Cantonal	Dr. José Gabriel Moreno
Director Dpto. Agua Potable	Ing. Kleber Padrón
Asesoría Jurídica	Dra. Delia Morales
Director del Dpto. de Avalúos y Catastros	Arq. Manuel Guzmán
Director Dpto. Administrativo	Ing. José Jacome
Jefe de Gestión Tecnológica	Ing. Luis Carrasco
Director Dpto. de Desarrollo de la Comunidad	Ab. Fernando Pico
Directora Dpto. Financiero	Lcda. Blanca Altamirano
Director Dpto. Obras Públicas	Ing. Roberto Aillón
Director Dpto. Orden y Control	Ing. Fausto Llerena
Director Dpto. de Planificación	Arq. Ernesto Morales
Registro de la Propiedad	Ab. Monserrath Trujillo
Director del Dpto. de Servicios Públicos	Ing. Daniel Oña

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

APRECIACIÓN DE LOS DEPARTAMENTOS: ORGANIZACIÓN FUNCIONAMIENTO

Al haber realizado la visita preliminar a las instalaciones del GADMCSPP, se pudo apreciar que la organización y cada uno de los departamentos están acordes a lo que indica el organigrama estructural. Además en cada departamento se observó la utilización de computadores de escritorio y en ciertos departamentos el uso de computadoras portátiles para el desarrollo de las actividades laborales.

Al mismo tiempo se pudo evidenciar que la mayoría de los computadores contaban con un regulador de voltaje, en caso de corte de energía, que les proporciona unos minutos para guardar la información de las actividades que realizaban en ese momento y posteriormente apagar el computador.

Además no todas las instalaciones son adecuadas para salvaguardar la seguridad física de los equipos informáticos debido a que se encontraban expuestos al sol y la humedad.

Mientras que en la Unidad a ser auditada se observó la falta de cámaras de seguridad o un registro para ingresar a la misma. Finalmente el centro de procesamiento de datos se encuentra en el mismo lugar de trabajo adaptado para su funcionamiento.

Elaborado Por:	JCVG	**Fecha:**	17-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-07-2018

ENTREVISTA AL JEFE DE LA UNIDAD DE GESTIÓN TECNOLÓGICA DEL GAD MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

Entrevistado: Ing. Luis Carrasco

1. **Cuántas personas trabajan en el área de sistemas y qué cargos desempeñan?**

Trabajan tres personas:

Jefe de la Unidad de Gestión Tecnológica

Técnico Profesional en Gestión Tecnológica (Redes)

Técnico Profesional en Gestión Tecnológica (Programación)

2. **Se ha establecido algún tipo de planificación para el área de sistemas?**

Si, el Plan Estratégico Informático y de Gobierno Electrónico período 2013- 2020

3. **Cuentan con planes de mantenimiento preventivo y correctivo de equipos informáticos, de redes y comunicaciones del Gobierno de San Pedro de Pelileo?**

Si, contamos con un plan de mantenimiento preventivo y correctivo establecido desde el 2014

4. **Cada qué tiempo se realiza el mantenimiento de los recursos informáticos?**

El mantenimiento se realiza cada año, además se realiza mantenimientos preventivos y correctivos.

5. **Existe alguna política para el uso de los recursos informáticos?**

Si, existe un reglamento que es de carácter obligatorio para todo el personal de la institución.

Elaborado Por:	JCVG	**Fecha:**	18-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	18-07-2018

6. Existe un inventario de los recursos informáticos y quien es el responsable de mantenerlo actualizado?

Si, existe un inventario y está a cargo del técnico profesional en gestión tecnológica.

7. Se realizan copias de los archivos en algún lugar distinto a los computadores?

Si, se realiza un almacenamiento externo y el respaldo de la información se realiza semanalmente.

8. Se ejecutaron los proyectos planteados en el POA 2016?

De los 8 proyectos que se plantearon en el POA 2016, se ejecutaron 6 durante el año, mientras que los proyectos como capacitación y licencia de firewall no se ejecutaron debido a la falta de presupuesto.

Elaborado Por:	JCVG	**Fecha:**	18-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	18-07-2018

4.2.2.2. Planificación Específica

MEMORÁNDUM DE PLANIFICACIÓN

Riobamba, 19 de julio de 2018

Entidad: GAD Municipal del Cantón San Pedro de Pelileo

Naturaleza del Trabajo: Auditoría Informática

Período: Del 1 de Enero al 31 de Diciembre de 2018

1. Motivo de la Auditoría

Se efectuará la Auditoría Informática a la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo con el fin de evaluar la seguridad de la información.

2. Objetivos de la Auditoría

Objetivo General

Realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, para evaluar la seguridad de la información.

Objetivos Específicos

- Analizar los riesgos que inciden en la seguridad de la información de la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.
- Identificar los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

Elaborado Por:	JCVG	**Fecha:**	19-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	19-07-2018

- Presentar el informe al concluir el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

3. Alcance de la Auditoría

El período que comprenderá la Auditoría Informática considera 1 de Enero al 31 de Diciembre del 2016.

4. Personal Encargado

Nombres	Cargo
Ing. Willian Yanza	Supervisor
Dr. Carlos Buenaño	Jefe de Equipo
Johanna Villena	Auditora

5. Plazo

El plazo estimado para la realización de la Auditoría Informática es de 65 días laborables.

6. Recursos a ser utilizados

Recursos Materiales

Cantidad	Detalle
7	Esferos azules
2	Esferos rojos
2	Lápices bicolores
1	Borrador
1	Sacapunta
1	Archivador
1	Resma de papel bond

Elaborado Por:	JCVG	**Fecha:**	19-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	19-07-2018

Recursos Tecnológicos

Cantidad	Detalle
2	Computadores portátiles
1	Calculadora
1	Escáner
1	Cámara digital

7. Metodología a utilizarse

La metodología para la realización de la Auditoría Informática serán:

- Observación directa
- Entrevistas al personal
- Cuestionarios de Control Interno COSO I

Atentamente,

Ing. Willian Yanza
SUPERVISOR

Dr. Carlos Buenaño
JEFE DE EQUIPO

Johanna Villena
AUDITORA

Elaborado Por:	JCVG	**Fecha:**	19-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	19-07-2018

Riobamba, 24 de Julio de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

De mi consideración:

De conformidad con la Orden de Trabajo N°001-FJVG-2018 con fecha 11 de julio de 2018, notificó a usted que la firma auditora "FENIX JVG AUDITORES & CONSULTORES ASOCIADOS", iniciará la Auditoría Informática en la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo, período comprendido entre el 01 de Enero y 31 de Diciembre de 2016. Además para ejecutar el trabajo de campo, hemos sido ilustrados para que establezcamos contacto con usted o con quien usted designe para la entrega de la documentación necesaria.

Por lo indicado solicito se sirva remitir la siguiente información:

- Misión y Visión Institucional
- Plan Estratégico Informático y de Gobierno Electrónico período 2013-2020
- POA 2016
- Reglamento para el uso de recursos informáticos, acceso a la red de datos e internet.
- Manuales de mantenimiento de los recursos informáticos.

Elaborado Por:	JCVG	**Fecha:**	24-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	24-07-2018

Cabe señalar que la información solicitada será tratada con absoluta confidencialidad y para los fines pertinentes a fin de ejecutar el trabajo de campo.

Sin otro particular, es propicia la oportunidad para reiterar mi más sincero agradecimiento.

Atentamente,

Ing. Willian Yanza
SUPERVISOR

Dr. Carlos Buenaño
JEFE DE EQUIPO

Johanna Villena
AUDITORA

Elaborado Por:	JCVG	**Fecha:**	24-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	24-07-2018

4.2.2.3. Ejecución de la Auditoría

Objetivo General:

Evaluar la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, mediante el análisis situacional y cuestionarios de control interno COSO I, para determinar la seguridad de la información.

Objetivos Específicos:

1. Analizar los riesgos que inciden en la seguridad de la información de la Unidad objeto de estudio.
2. Identificar los procesos que realiza la Unidad objeto de estudio.

N°	Procedimiento	Referencia P/T	Elaborado por	Fecha
1	Elabore el Programa de Auditoria	P/A 1/2	JCVG	25-07-2018
2	Realice el Análisis Situacional FODA	A/S 1/2	JCVG	26-07-2018
3	Realice la Matriz de Correlación FO	MC/FO 1/1	JCVG	27-07-2018
4	Realice la Matriz de Correlación DA	MC/DA 1/2	JCVG	30-07-2018
5	Realice el Perfil Estratégico Interno	PE/I 1/2	JCVG	31-07-2018
6	Realice el Perfil Estratégico Externo	PE/E 1/2	JCVG	01-08-2018
7	Elabore los Cuestionarios de Control Interno (Check List) aplicando el COSO I	C/CI 1/14	JCVG	02-08-2018 08-08-2018
8	Realice la Matriz Resumen de Cuestionarios de Control Interno	MR/CCI 1/1	JCVG	09-08-2018
9	Elabore la Hoja de Hallazgos	H/H 1/11	JCVG	13-08-2018 17-08-2018
10	Elabore la Hoja de Indicadores	H/I 1/6	JCVG	20-08-2018 23-08-2018
11	Revise la Hoja del POA 2016	H/POA 1/8	JCVG	24-08-2018

Elaborado Por:	JCVG	**Fecha:**	25-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	26-07-2018

N°	Procedimiento	Referencia P/T	Elaborado por	Fecha
12	Determine los Factores de Riesgo	**F/R 1/1**	JCVG	27-08-2018
13	Verifique el Inventario de Hardware	**I/HW 1/32**	JCVG	27-08-2018 03-09-2018
14	Verifique el Inventario de Software	**I/SW 1/1**	JCVG	04-09-2018

Elaborado Por:	JCVG	**Fecha:**	25-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	26-07-2018

ANÁLISIS INTERNO			
FORTALEZAS		**DEBILIDADES**	
F1	Personal con experiencia en aspectos funcionales en informática	**D1**	El presupuesto asignado para algunos proyectos puede resultar escaso
F2	Prestigio ganado entre otras instituciones y en la opinión pública como una Municipalidad con interés y experiencia en el uso de las herramientas del Gobierno Electrónico	**D2**	Existencia de un grupo de equipos de cómputo obsoletos
F3	La institución cuenta con el comité informático institucional	**D3**	Déficit de equipos de cómputo y UPS con regulador de voltaje
F4	Utilización de las nuevas tecnologías de la información y comunicaciones (TIC) para proveer servicios electrónicos a los ciudadanos a través del Balcón de Servicios	**D4**	No existe un control de ingreso al área de sistemas a personas no autorizadas
F5	Impulso por parte de la Alta Dirección al tema de Gobierno Electrónico	**D5**	Deficiencia de personal para el área de gestión tecnológica

Elaborado Por:	JCVG	**Fecha:**	26-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	27-07-2018

ANÁLISIS EXTERNO			
OPORTUNIDADES		**AMENAZAS**	
O1	Mayor utilización de las nuevas tecnologías de la información y comunicaciones (TIC) (Era Digital)	**A1**	Desastres como incendios
O2	Composición demográfica y socioeconómica adecuada para la implementación de soluciones en materia de Gobierno Electrónico	**A2**	Institución de alta visibilidad, propensa a intentos de ser atacados (hacker o cracker)
O3	Nuevas herramientas que permiten virtualizar servidores y computadoras	**A3**	Virus Informáticos
O4	Apoyo de ONGs y AME para la implementación de Gobierno Electrónico	**A4**	Cortes de Energía en todo el Cantón

ANÁLISIS:

El GAD Municipal del Cantón San Pedro de Pelileo, con respecto al uso de las Tecnologías de la Información y Comunicación (TIC) presenta diversas fortalezas y debilidades en el ámbito interno, que fueron analizadas mediante indagación y apreciación del personal de la Unidad de Gestión Tecnológica, además de oportunidades que deben ser aprovechadas y amenazas que con el tiempo deben ser erradicadas.

Además cabe señalar que el Gobierno Electrónico, no es más que el uso de las tecnologías de la información por parte de las entidades del Estado en el cumplimiento de sus diversas funciones y actividades.

Elaborado Por:	JCVG	**Fecha:**	26-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	27-07-2018

		O1	O2	O3	O4		
	FO	Mayor utilización de las nuevas tecnologías de la información y comunicaciones (TIC) (Era Digital)	Composición demográfica y socioeconómica adecuada para la implementación de soluciones en materia de Gobierno Electrónico	Nuevas herramientas que permiten virtualizar servidores y computadoras	Apoyo de ONGs y AME para la implementación de Gobierno Electrónico	**TOTAL**	
F1	Personal con experiencia en aspectos funcionales en informática	5	1	5	5	**16**	**19%**
F2	Prestigio ganado entre otras instituciones y en la opinión pública como una Municipalidad con interés y experiencia en el uso de las herramientas del Gobierno Electrónico	5	3	5	5	**18**	**21%**
F3	La institución cuenta con el comité informático institucional	5	3	5	3	**16**	**19%**
F4	Utilización de las nuevas tecnologías de la información y comunicaciones (TIC) para proveer servicios electrónicos a los ciudadanos a través del Balcón de Servicios	5	3	5	5	**18**	**21%**
F5	Impulso por parte de la Alta Dirección al tema de Gobierno Electrónico	5	3	5	5	**18**	**21%**
	TOTAL	**25**	**13**	**25**	**23**	**86**	**100%**
		29%	**15%**	**29%**	**27%**	**100%**	

Para la ponderación se tomó en cuenta la siguiente escala:

Si la relación es significativa directa entre F y O = 5
Si la relación es media entre F y O = 3
Si no tiene relación entre F y O = 1

ANÁLISIS: La Matriz de Correlación FO denota un alto porcentaje del 21% con respecto al prestigio, utilización de las TIC para ofrecer servicios, impulso del Gobierno Electrónico, mientras que las oportunidades con mayor porcentaje del 29% corresponde al mayor uso de las TIC y las nuevas herramientas que permiten virtualizar servidores y computadoras.

Elaborado Por:	JCVG	**Fecha:**	27-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	30-07-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Matriz de Correlación DA** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI MC/ DA 1/1**

		A1	A2	A3	A4		
	DA	Desastres como incendios	Institución de alta visibilidad, propensa a intentos de ser atacados (hacker o cracker)	Virus Informáticos	Cortes de Energía en todo el Cantón	**TOTAL**	
D1	El presupuesto asignado para algunos proyectos puede resultar escaso	3	5	5	1	**14**	**28%**
D2	Existencia de un grupo de equipos de cómputo obsoletos	1	1	5	3	**10**	**20%**
D3	Déficit de equipos de cómputo y UPS con regulador de voltaje	1	1	5	5	**12**	**24%**
D4	No existe un control de ingreso al área de sistemas a personas no autorizadas	1	3	3	1	**8**	**16%**
D5	Deficiencia de personal para el área de gestión tecnológica	1	1	3	1	**6**	**12%**
	TOTAL	**7**	**11**	**21**	**11**	**50**	**100%**
		14%	**22%**	**42%**	**22%**	**100%**	

Para la ponderación se tomó en cuenta la siguiente escala:

Si la relación es significativa directa entre D y A = 5
Si la relación es media entre D y A = 3
Si no tiene relación entre D y A = 1

ANÁLISIS: La Matriz de Correlación DA denota un alto porcentaje del 28% con respecto al escaso presupuesto asignado, mientras que las amenazas con un porcentaje del 22% se refieren a los ataques cibernéticos y los cortes de energía que afectan debido a los falta de seguridad física y lógica de los equipos a esto va ligado con un porcentaje de 42% los virus informáticos.

Elaborado Por:	JCVG	**Fecha:**	30-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	31-07-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Perfil Estratégico Interno** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI PE/I 1/2**

ASPECTOS INTERNOS		CLASIFICACION /IMPACTO				
		DEBILIDAD		EQUILIBRIO	FORTALEZA	
		Gran Debilidad	Debilidad		Fortaleza	Gran Fortaleza
D1	El presupuesto asignado para algunos proyectos puede resultar escaso					
D2	Existencia de un grupo de equipos de cómputo obsoletos					
D3	Déficit de equipos de cómputo y UPS con regulador de voltaje					
D4	No existe un control de ingreso al área de sistemas a personas no autorizadas					
D5	Deficiencia de personal para el área de gestión tecnológica					
F1	Personal con experiencia en aspectos funcionales en informática					
F2	Prestigio ganado entre otras instituciones y en la opinión pública como una Municipalidad con interés y experiencia en el uso de las herramientas del Gobierno Electrónico					
F3	La institución cuenta con el comité informático institucional					
F4	Utilización de las nuevas tecnologías de la información y comunicaciones (TIC) para proveer servicios electrónicos a los ciudadanos a través del Balcón de Servicios					
F5	Impulso por parte de la Alta Dirección al tema de Gobierno Electrónico					
	TOTAL	1	4	0	4	1
	PORCENTAJE	**20.00%**	**80.00%**		**80.00%**	**20.00%**

Elaborado Por:	JCVG	**Fecha:**	31-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	31-07-2018

ANÁLISIS:

Como se puede observar el Perfil Estratégico Interno con respecto a la mayor debilidad que posee la Unidad de Gestión Tecnológica es la falta de presupuesto, mientras que la mayor fortaleza es el prestigio que tiene ante el resto de instituciones, en cuanto al uso de las herramientas del Gobierno Electrónico.

Elaborado Por:	JCVG	**Fecha:**	31-07-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	31-07-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Perfil Estratégico Externo** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI PE/E 1/2**

ASPECTOS EXTERNOS		**CLASIFICACION /IMPACTO**				
		AMENAZAS		**EQUILIBRIO**	**OPORTUNIDAD**	
		Gran Amenaza	**Amenaza**		**Oportunidad**	**Gran Oportunidad**
A1	Desastres como incendios					
A2	Institución de alta visibilidad, propensa a intentos de ser atacados (hacker o cracker)					
A3	Virus Informáticos					
A4	Cortes de Energía en todo el Cantón					
O1	Mayor utilización de las nuevas tecnologías de la información y comunicaciones (TIC) (Era Digital)					
O2	Composición demográfica y socioeconómica adecuada para la implementación de soluciones en materia de Gobierno Electrónico					
O3	Nuevas herramientas que permiten virtualizar servidores y computadoras					
O4	Apoyo de ONGs y AME para la implementación de Gobierno Electrónico					
	TOTAL	2	2	0	3	1
	PORCENTAJE	**50%**	**50%**		**75%**	**25%**

Elaborado Por:	JCVG	**Fecha:**	01-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	01-08-2018

ANÁLISIS:

Como se puede observar en el Perfil Estratégico Externo las mayores amenazas son los ataques por hacker o cracker, así como los virus informáticos. Además la oportunidad más representativa se refiere a la mayor utilización de las nuevas tecnologías de la información y comunicaciones (TIC) Era Digital, lo que facilita la interacción con los usuarios.

Elaborado Por:	JCVG	**Fecha:**	01-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	01-08-2018

Componente:		**Ambiente de Control**			
N°	**PREGUNTA**	**RESPUESTA**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	El Organigrama de la Institución define los niveles de apoyo y asesoría para Gestión Tecnológica?		x		La Unidad de Gestión Tecnológica es dependiente de la Dirección Administrativa *
2	El personal que labora en la Unidad de Gestión Tecnológica cumple con el perfil de puestos?	x			Ingenieros en Sistemas Informáticos
3	El personal de la Unidad de Gestión Tecnológica participa en los programas de capacitación institucionales?	x			
4	Cuentan con el Plan Estratégico Informático?	x			
5	El Plan Estratégico Informático se encuentra actualizado?		x		El Plan Estratégico Informático no se encuentra actualizado desde el 2013 que fue creado con vigencia al 2020 *
6	El personal ejerce un control interno basado en las Normas de Control Interno de la CGE?	x			
7	El personal conoce y aplica las Norma de Control Interno 410 con respecto a la Tecnología de la Información?	x			
8	Existe un reglamento para el uso de los recursos informáticos?	x			
	TOTAL	6	2		

Elaborado Por:	JCVG	**Fecha:**	02-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

TOTAL RESPUESTAS	
POSITIVAS	6
NEGATIVAS	2
TOTAL	**8**

$$\textbf{Nivel de Confianza} = \frac{\textbf{Respuestas Positivas}}{\textbf{Total de Respuestas}} x\ 100$$

$$\textbf{Nivel de Confianza} = \frac{6}{8}\ x100$$

$$\textbf{Nivel de Confianza} = 75\%$$

$$\textbf{Nivel de Riesgo} = \textbf{100}\ \% - \textbf{Nivel de Confianza}$$

$$\textbf{Nivel de Riesgo} = 100\ \% - 75\%$$

$$\textbf{Nivel de Riesgo} = 25\%$$

NIVEL DE RIESGO		
ALTO	MEDIO	BAJO
85% - 51%	50% - 36%	35% - 5%-0%
NIVEL DE CONFIANZA		
15% - 50%	51% - 79%	80% - 95%-100%
BAJO	MEDIO	ALTO

Interpretación:

Los resultados de los Cuestionarios de Control Interno sobre el componente "Ambiente de Control" son: Nivel de Confianza 75% que representa un nivel medio, mientras que el Nivel de Riesgo del 25% lo que representa un nivel bajo, que significa que los ítems analizados tienen un impacto parcial sobre las actividades institucionales.

Elaborado Por:	JCVG	**Fecha:**	02-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Componente:		**Evaluación de riesgos**			
N°	**PREGUNTA**	**RESPUESTA**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
9	La máxima autoridad y el personal de la Unidad de Gestión Tecnológica han identificado los factores que pueden ocasionar la ocurrencia de riesgos informáticos?	x			
10	El personal de la UGT conjuntamente con la Unidad de Gestión de Riesgos han definido mecanismos para mitigar posibles riesgos que afecten a los equipos informáticos?	x			
11	La Unidad de Gestión Tecnológica posee extintores en caso de incendios? Cuántos? Y de qué tipo?	x			Existen dos extintores de tipo CO2 y Polvo químico
12	Se realizan respaldos de la información de la institución en caso de que se susciten desastres que puedan afectar los equipos informáticos?	x			
	TOTAL	4	0		

Elaborado Por:	JCVG	**Fecha:**	02-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

TOTAL RESPUESTAS	
POSITIVAS	4
NEGATIVAS	0
TOTAL	**4**

$$\textbf{Nivel de Confianza} = \frac{\textbf{Respuestas Positivas}}{\textbf{Total de Respuestas}} x\ \mathbf{100}$$

$$\textbf{Nivel de Confianza} = \frac{4}{4}\ x100$$

$$\textbf{Nivel de Confianza} = 100\%$$

$$\textbf{Nivel de Riesgo} = \mathbf{100}\ \% - \textbf{Nivel de Confianza}$$

$$\textbf{Nivel de Riesgo} = 100\ \% - 100\%$$

$$\textbf{Nivel de Riesgo} = 0\%$$

NIVEL DE RIESGO		
ALTO	**MEDIO**	**BAJO**
85% - 51%	50% - 36%	35% - 5%-0%
NIVEL DE CONFIANZA		
15% - 50%	51% - 79%	80% - 95%-100%
BAJO	**MEDIO**	**ALTO**

Interpretación:

Los resultados de los Cuestionarios de Control Interno sobre el componente "Evaluación del Riesgo" son: Nivel de Confianza 100% que representa un nivel alto, mientras que el Nivel de Riesgo es 0% lo que representa un nivel bajo, que significa que los ítems analizados no tienen un impacto representativo en las actividades de la institución.

Elaborado Por:	JCVG	**Fecha:**	02-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Componente:		**Actividades de Control**			
N°	**PREGUNTA**	**RESPUESTA**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
Seguridad Física					
13	El acceso a la Unidad de Gestión Tecnológica se encuentra restringido para el personal no autorizado?		x		El acceso no se encuentra restringido para el personal no autorizado *
14	La Unidad de Gestión Tecnológica cuenta con una salida de emergencia?	x			
15	La Unidad de Gestión Tecnológica cuenta con señalética suficiente?		x		La señalética de la Unidad de Gestión Tecnológica no es suficiente*
16	La iluminación del área es adecuada?	x			
17	La instalación física de la Unidad de Gestión Tecnológica está libre de goteras en caso de temporada de lluvias?		x		La Unidad de Gestión Tecnológica presenta daños en los techos lo que puede provocar goteras en temporadas de lluvia *
18	La Unidad de Gestión Tecnológica cuenta con cámaras de seguridad?		x		La Unidad no cuenta con cámaras de seguridad *
19	El personal de la Unidad de Gestión Tecnológica realiza las bitácoras con respecto al uso de los equipos informáticos?	x			
20	Se ha establecido un Comité Informático Institucional? Quiénes lo integran? Cada qué tiempo se reúne?	x			El Comité Informático Institucional está conformado por 5 miembros: Jefe de Sistemas, los dos técnicos del área de sistemas, Responsable de Gestión de Riesgo, Responsable de Compras Públicas

Elaborado Por:	JCVG	**Fecha:**	03-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

N°	PREGUNTA	RESPUESTA			OBSERVACIONES
		SI	NO	N/A	
21	El Centro de Procesamiento de Datos se encuentra ubicado en un lugar externo?		x		El Centro de Procesamiento de Datos se encuentra en el área de sistemas en un sección dividida por lo que genera ruido *
22	El Centro de Procesamiento de Datos y los equipos informáticos cuentan con una póliza de seguros que los cubra en caso de suscitarse algún desastre?		x		El CPD y los equipos informáticos no poseen una póliza de seguros *
23	El Centro de Procesamiento de Datos dispone de aire de precisión para regular la temperatura?	x			
24	Los puntos del Centro de Procesamiento de Datos está debidamente aterrizados (conexión a tierra)?	x			
25	Los computadores se encuentran conectados a una red? Qué tipo de red existe y qué dirección IP tiene?	x			Red LAN y la dirección IP 192
26	La red se encuentra funcionando con cableado estructurado certificado? Y bajo que norma?	x			Norma ANSI EIA/TIA-568-B
27	El área cuenta con planos de los puntos de red?	x			
28	Existen planos de la instalación eléctrica?	x			

Elaborado Por:	JCVG	**Fecha:**	03-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

N°	PREGUNTA	RESPUESTA			OBSERVACIONES
		SI	NO	N/A	
29	El Centro de Procesamiento de Datos dispone de un UPS para protección de datos? Cuánto tiempo?	x			Dispone de 6000 volts/amperios (1hora)
30	Los equipos de cómputo disponen de un UPS para protección de datos? Cuánto tiempo?	x			La mayoría de equipos de cómputo disponen de un UPS para la protección de datos para 10 minutos en los que se puede salvaguardar la información
31	Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?	x			
32	Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores de pico, generadores de energía, UPS con regulador de voltaje?	x			
33	Existe redundancia eléctrica implementada?	x			
34	Existe redundancia en el almacenamiento de datos?	x			
35	La infraestructura de red dispone de racks por piso?	x			
36	El lugar de la Unidad de Gestión Tecnológica cuenta con sensores de humo?	x			

Elaborado Por:	JCVG	**Fecha:**	03-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

N°	PREGUNTA	RESPUESTA			OBSERVACIONES
		SI	NO	N/A	
37	Se realizan mantenimientos preventivos a los equipos informáticos institucionales? Cada qué tiempo?	x			Se realizan mantenimientos preventivos semestrales los días Lunes y Viernes (2 equipos por día) en un mes se realizan 16 mantenimientos preventivos
38	Se realizan mantenimientos correctivos a los equipos informáticos institucionales? Cada qué tiempo?	x			Se realizan mantenimientos correctivos semestrales
39	La instalación y/o mantenimiento se realiza de manera planificada y organizada? Cómo se realiza?	x			Se realiza dentro del horario de trabajo si se evidencian daños o falencias que impiden el desarrollo normal de las actividades y se realiza fuera del horario de trabajo en caso de ser necesario
40	Se actualiza el inventario de los equipos informáticos? Quién es el responsable? Cada qué tiempo se actualiza?	x			El técnico del área es el encargado de mantener actualizados anualmente los inventarios de los equipos informáticos
41	Existen políticas para adquisición de equipos informáticos de forma estandarizada?	x			Los equipos informáticos estandarizados son: computadores marca HP, portátiles marca Toshiba, impresoras marca EPSON, proyectores marca EPSON y copiadoras marca Xerox y Ricoh, Switch normales de capa 2 [CISCO] y Switch POE de capa 2 [HP]
42	Existen procedimientos para dar de baja los equipos informáticos obsoletos?		x		No existe una procedimiento específicos para dar de baja los equipos informáticos obsoletos, son llevados a la bodega *

Elaborado Por:	JCVG	**Fecha:**	03-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

N°	PREGUNTA	RESPUESTA			OBSERVACIONES
		SI	NO	N/A	
43	Se utilizan firmas electrónicas en la Institución?	x			Existe un contrato con vigencia de dos años
Seguridad Lógica					
44	Los respaldos de la información obtenidos son almacenados en la nube para mayor seguridad?	x			Los respaldos de información se realizan semanalmente
45	La institución utiliza servicios de empresas que almacenan la información en diferentes sitios o ciudades del país?		x		Los respaldos de la información no son guardados en algún sitio o ciudad del país *
46	Existe un documento formal que establezca el uso y cambio de contraseñas fuertes dirigido a los servidores/as del GAD Municipal del Cantón San Pedro de Pelileo?	x			
47	Los Funcionarios del GAD Municipal del Cantón San Pedro de Pelileo cumplen con uso y cambio de contraseñas fuertes de acuerdo al documento formal establecido?		x		Los funcionarios no poseen contraseñas fuertes de acuerdo a lo que señala el documento formal establecido *
48	Se actualiza el antivirus de los equipos informáticos a fin de evitar pérdida de información?	x			
49	Los equipos informáticos poseen las aplicaciones necesarias para que los servidores/as puedan cumplir con sus actividades laborales diarias?	x			
	TOTAL	28	9		

Elaborado Por:	JCVG	**Fecha:**	06-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

TOTAL RESPUESTAS	
POSITIVAS	28
NEGATIVAS	9
TOTAL	37

$$\textbf{Nivel de Confianza} = \frac{\textbf{Respuestas Positivas}}{\textbf{Total de Respuestas}} x\ \mathbf{100}$$

$$\textbf{Nivel de Confianza} = \frac{28}{37}\ x100$$

$$\textbf{Nivel de Confianza} = 76\%$$

$$\textbf{Nivel de Riesgo} = \mathbf{100}\ \% - \textbf{Nivel de Confianza}$$

$$\textbf{Nivel de Riesgo} = 100\ \% - 76\%$$

$$\textbf{Nivel de Riesgo} = 24\%$$

NIVEL DE RIESGO		
ALTO	MEDIO	BAJO
85% - 51%	50% - 36%	35% - 5%-0%
NIVEL DE CONFIANZA		
15% - 50%	51% - 79%	80% - 95%-100%
BAJO	MEDIO	ALTO

Interpretación:

Los resultados de los Cuestionarios de Control Interno sobre el componente "Actividades de Control" son: Nivel de Confianza 76% que representa un nivel medio, mientras que el Nivel de Riesgo del 24% lo que representa un nivel bajo, que significa que los ítems analizados tienen un impacto parcial sobre las actividades institucionales.

Elaborado Por:	JCVG	**Fecha:**	06-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Componente:		**Información y Comunicación**			
N°	**PREGUNTA**	**RESPUESTA**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
50	La máxima autoridad y niveles de dirección comunican oportunamente la información a los servidores/as para el cumplimiento de sus funciones?	x			
51	El sistema de información y comunicación registra, procesa, resume e informa sobre las operaciones técnicas y financieras de la institución?	x			
52	El sistema de información y comunicación cuenta con los controles necesarios que garanticen la confiabilidad, seguridad con respecto a la información?	x			
53	La institución ha establecido canales de comunicación que permitan trasladar la información de forma segura, correcta y oportuna hacia los servidores/as?	x			
54	El sistema de información computarizado responde a las necesidades de la institución y normal desarrollo de las actividades de los servidores/as?	x			
55	Los servidores/as poseen un correo institucional?	x			
56	La institución posee diferentes servidores de datos? Cuáles?	x			Servidor Alfanumérico y Gráfico, Servidor de Aplicaciones, Servidor de Pruebas, Servidor de Internet
	TOTAL	7	0		

Elaborado Por:	JCVG	**Fecha:**	07-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

TOTAL RESPUESTAS	
POSITIVAS	7
NEGATIVAS	0
TOTAL	7

$$\textbf{Nivel de Confianza} = \frac{\textbf{Respuestas Positivas}}{\textbf{Total de Respuestas}} x\ 100$$

$$\textbf{Nivel de Confianza} = \frac{7}{7}\ x100$$

$$\textbf{Nivel de Confianza} = 100\%$$

$$\textbf{Nivel de Riesgo} = \textbf{100}\ \% - \textbf{Nivel de Confianza}$$

$$\textbf{Nivel de Riesgo} = 100\ \% - 100\%$$

$$\textbf{Nivel de Riesgo} = 0\%$$

NIVEL DE RIESGO		
ALTO	MEDIO	BAJO
85% - 51%	50% - 36%	35% - 5%-0%
NIVEL DE CONFIANZA		
15% - 50%	51% - 79%	80% - 95%-100%
BAJO	MEDIO	ALTO

Interpretación:

Los resultados de los Cuestionarios de Control Interno sobre el componente "Información y Comunicación" son: Nivel de Confianza 100% que representa un nivel alto, mientras que el Nivel de Riesgo es 0% lo que representa un nivel bajo, que significa que los ítems analizados no tienen un impacto representativo en las actividades de la institución.

Elaborado Por:	JCVG	**Fecha:**	07-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Componente:		**Supervisión o Monitoreo**			
N°	**PREGUNTA**	**RESPUESTA**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
57	Existe un control sobre el uso y buen funcionamiento de los equipos informáticos institucionales?	**x**			El control y monitoreo se coordina con los usuarios a fin de tener la disponibilidad de los equipos sin afectar las labores cotidianas.
58	El personal de la Unidad de Gestión Tecnológica elabora un Informe Técnico sobre el estado de los equipos informáticos institucionales?	**x**			
59	Se asigna un custodio para cada uno de los equipos informáticos que son utilizados en el lugar de trabajo?	**x**			
60	Se verifica el buen estado de las instalaciones eléctricas y puntos de red?	**x**			
61	El Jefe de Gestión Tecnológica se encarga de supervisar las actividades realizadas por los técnicos de área?	**x**			
	TOTAL	5	0		

TOTAL RESPUESTAS	
POSITIVAS	5
NEGATIVAS	0
TOTAL	**5**

Elaborado Por:	JCVG	**Fecha:**	08-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

$$\textbf{Nivel de Confianza} = \frac{\textbf{Respuestas Positivas}}{\textbf{Total de Respuestas}} x\ \mathbf{100}$$

$$\textbf{Nivel de Confianza} = \frac{5}{5}\ x100$$

$$\textbf{Nivel de Confianza} = 100\%$$

$$\textbf{Nivel de Riesgo} = \mathbf{100}\ \% - \textbf{Nivel de Confianza}$$

$$\textbf{Nivel de Riesgo} = 100\ \% - 100\%$$

$$\textbf{Nivel de Riesgo} = 0\%$$

NIVEL DE RIESGO		
ALTO	**MEDIO**	**BAJO**
85% - 51%	50% - 36%	35% - 5%-0%
NIVEL DE CONFIANZA		
15% - 50%	51% - 79%	80% - 95%-100%
BAJO	**MEDIO**	**ALTO**

Interpretación:

Los resultados de los Cuestionarios de Control Interno sobre el componente "Supervisión o Monitoreo" son: Nivel de Confianza 100% que representa un nivel alto, mientras que el Nivel de Riesgo es 0% lo que representa un nivel bajo, que significa que los ítems analizados no tienen un impacto representativo en las actividades de la institución.

Elaborado Por:	JCVG	**Fecha:**	08-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

FÉNIX IVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Matriz Resumen de Cuestionarios de Control Interno** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI** **MR/CCI** **1/1**

MATRIZ RESUMEN DE CUESTIONARIOS DE CONTROL INTERNO								
N°	**Componente**	**Referencia P/T**	**% Confianza**	**Nivel de Confianza**		**% Riesgo**	**Nivel de Riesgo**	
1	Ambiente de Control	EAI CC/I 2/14	75		Medio	25		Bajo
2	Evaluación de Riesgos	EAI CC/I 4/14	100		Alto	0		Bajo
3	Actividades de Control	EAI CC/I 10/14	76		Alto	24		Bajo
4	Información y Comunicación	EAI CC/I 12/14	100		Alto	0		Bajo
5	Supervisión o Monitoreo	EAI CC/I 14/14	100		Alto	0		Bajo
Total			451			49		
Promedio			90.20		Alto	9.80		Bajo

Interpretación:

Como se puede observar en la Matriz Resumen el nivel de confianza es Alto con un promedio de 90,20 y el nivel de riesgo es bajo con un promedio de 9,80. Sin embargo en la matriz se puede observar en los componentes Ambiente de Control y Actividades de Control un nivel de confianza medio, esto se debe a que existen actividades que provocan un impacto moderado y deben ser tomadas en cuenta por las autoridades.

Elaborado Por:	JCVG	**Fecha:**	09-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	03-10-2018

La Unidad de Gestión Tecnológica depende de la Dirección Administrativa
Condición
La Unidad de Gestión Tecnológica es dependiente de la Dirección Administrativa
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-01 Organización Informática señala: La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuaria; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.
Causa
La Unidad de Gestión Tecnológica realiza las actividades de asesoría y apoyo tecnológico bajo la responsabilidad de la Dirección Administrativa
Efecto
Los procesos tardan debido a que se debe esperar el visto bueno de la Dirección Administrativa
Conclusión
La Unidad de Gestión Tecnológica al ser dependiente de la Dirección Administrativa provoca que los procesos tarden hasta esperar su aprobación de acuerdo a los trámites que realizan las diferentes unidades pertenecientes a la misma dirección, por lo que no se cumple con la Norma Técnica de Control Interno de la CGE, 410-01 Organización Informática.
Recomendación
Se recomienda al Alcalde y Concejo Municipal posicionar a Gestión Tecnológica en un nivel directivo independiente a fin que le permita efectuar las actividades de asesoría, apoyo y ayudar en la toma de decisiones organizacionales.

Elaborado Por:	JCVG	**Fecha:**	13-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Plan Estratégico Informático desactualizado
Condición
El Plan Estratégico Informático no se encuentra actualizado desde el 2013 que fue creado con vigencia al 2020
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-03 Plan informático estratégico de tecnología señala: La Unidad de Tecnología de la Información elaborará e implementará un plan informático estratégico, así como planes operativos y el presupuesto asociado, se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.
Causa
El Plan Estratégico Informático fue creado con vigencia hasta el año 2020 por lo que no se ha requerido actualizar permanentemente ni periódicamente.
Efecto
La información que proporciona el Plan Estratégico Informático no proporciona la realidad del área y del Gobierno Electrónico de la institución.
Conclusión
El Plan Estratégico Informático no brinda información actualizada por lo que se convierte en un instrumento no válido a la hora de tomar decisiones, además no se cumple con la Norma Técnica de Control Interno de la CGE, 410-03 Plan informático estratégico
Recomendación
Se recomienda al Jefe de Gestión Tecnológica actualizar periódicamente el Plan Estratégico Informático de la Institución con el fin de proporcionar información veraz acerca del Gobierno Electrónico de GAD Municipal del Cantón San Pedro de Pelileo.

Elaborado Por:	JCVG	**Fecha:**	13-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Falta de control de acceso a la Unidad de Gestión Tecnológica
Condición
El acceso a la Unidad de Gestión Tecnológica no se encuentra restringido para el personal no autorizado
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-10 Seguridad de tecnología de información señala: la Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas: Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas.
Causa
Por lo general en el lugar se encuentra una persona con el fin de controlar y atender a los usuarios que lo requieran, sin embargo si deben salir todos los técnicos y el jefe se mantiene la puerta cerrada con seguro.
Efecto
La falta de control de acceso a personas no autorizadas y ajenas a la Unidad de Gestión Tecnológica puede provocar pérdidas de herramientas y objetos de la unidad, por lo que significaría incurrir en gastos adicionales para sustituir las herramientas faltantes. Además se debe considerar la sustracción de información confidencial.
Conclusión
La Unidad de Gestión Tecnológica no posee un control de acceso para el personal no autorizado lo que provocaría la pérdida de herramientas y el robo de la información, incumpliendo con lo que estipula la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.
Recomendación
Se recomienda el Jefe de la Unidad de Gestión Tecnológica controlar el acceso de personal no autorizado, mediante registros e identificaciones.

Elaborado Por:	JCVG	**Fecha:**	14-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Señalética Insuficiente
Condición
La señalética de la Unidad de Gestión Tecnológica no es suficiente
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-09 Mantenimiento y control de la infraestructura tecnológica señala: La Unidad de Tecnología de Información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.
Causa
La falta de presupuesto para implementar la señalética suficiente en la Unidad.
Efecto
Desinformación de usuarios internos y externos.
Conclusión
La señalética de la Unidad al ser insuficiente provoca desinformación entre los usuarios tanto internos como externos, debido a la falta de presupuesto por lo que se debe solicitar en el POA para los siguientes años y cumplir con la Norma Técnica de Control Interno de la CGE, 410-09 Mantenimiento y control de la infraestructura tecnológica.
Recomendación
Se recomienda al Jefe de la Unidad de Gestión Tecnológica implementar en el POA la señalética que se requiere para la unidad.

Elaborado Por:	JCVG	**Fecha:**	14-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Daños en el techo de la Unidad de Gestión Tecnológica
Condición
La Unidad de Gestión Tecnológica presenta daños en los techos lo que puede provocar goteras en temporadas de lluvia
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-10 Seguridad de tecnología de información señala: la Unidad de Tecnología de Información contará con instalaciones físicas adecuadas.
Causa
La Unidad se encuentra ubicada en el primer piso del edificio nuevo por lo que tenía proyección a dos pisos, el cual no llego a concluirse, por esta razón se filtra el agua en temporada de lluvias fuertes.
Efecto
Filtraciones de agua en el techo del edificio nuevo que pueden dañar los equipos informáticos institucionales.
Conclusión
Las filtraciones de agua existentes en el edificio nuevo en donde se encuentra ubicada la Unidad de Gestión Tecnológica pueden llegar a dañar los equipos informáticos institucionales , debido a que no se consideró la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.
Recomendación
Se recomienda al Sr. Alcalde y al Jefe de la Unidad de Gestión Tecnológica tomar las respectivas medidas para evitar que las filtraciones de agua lleguen a dañar los equipos informáticos institucionales.

Elaborado Por:	JCVG	**Fecha:**	15-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Inexistencia de cámaras de seguridad en la Unidad de Gestión Tecnológica
Condición
La Unidad de Gestión Tecnológica no cuenta con cámaras de seguridad
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-10 Seguridad de tecnología de información señala: la Unidad de Tecnología de Información se encargará de la implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
Causa
Por falta de presupuesto no se ha implementado un sistema de seguridad de cámaras de vigilancia para la Unidad.
Efecto
No existe monitoreo de actividades e ingreso de personal no autorizado a la Unidad incidiendo en pérdidas de los equipos informáticos y herramientas.
Conclusión
La Unidad de Gestión Tecnológica cuenta con cámaras de seguridad por lo que incide en la pérdida de equipos informáticos y herramientas e incumpliendo con la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.
Recomendación
Se recomienda al Jefe de la Unidad de Gestión Tecnológica formular un proyecto para la implementación de cámaras de vigilancia para garantizar la seguridad física interna e implementar en el POA para los próximos años.

Elaborado Por:	JCVG	**Fecha:**	15-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Ubicación del Centro de Procesamiento de Datos
Condición
El Centro de Procesamiento de Datos se encuentra adecuada en el área de sistemas en un sección dividida por lo que genera ruido
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-08 Adquisición de infraestructura tecnológica señala: La Unidad de Tecnología de Información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.
En este caso el estándar internacional que sirve de guía para el diseño e instalación de centros de datos se denomina ANSI-TIA 942 que define los TIER al indicar niveles de fiabilidad en función del nivel de la disponibilidad. Además otro estándar a ser implementado es la Norma ISO 27001 que gestiona la seguridad de la información en una entidad.
Causa
Escaso presupuesto para que el Centro de Procesamiento de Datos se encuentre propicio a estándares
Efecto
Reducción del área de trabajo y uso de espacios que no están habilitados para el funcionamiento del Centro de Procesamiento de Datos.
Conclusión
El área en donde se encuentra el Centro de Procesamiento de Datos está adecuada de acuerdo al presupuesto asignado por lo que reduce el espacio y el personal que labora en dicha área debe adaptarse al ruido que genera y no se cumple con la Norma Técnica de Control Interno de la CGE, 410-08 Adquisición de infraestructura tecnológica.
Recomendación
Se recomienda al Sr. Alcalde y al Jefe de la Unidad de Gestión Tecnológica tomar las respectivas medidas para propiciar una infraestructura adecuada para el Centro de Procesamiento de Datos a fin de salvaguardar la integridad, confiabilidad y disponibilidad de la información institucional.

Elaborado Por:	JCVG	**Fecha:**	16-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Pólizas de seguros para el Centro de Procesamiento de Datos y equipos informáticos
Condición
El Centro de Procesamiento de Datos y los equipos informáticos no poseen una póliza de seguros
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-10 Seguridad de tecnología de información señala: la Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos
Causa
Al comprar los equipos para la institución no solicitan la respectiva póliza de seguros que los cubran en casos fortuitos
Efecto
Si ocurre un caso fortuito que dañe los equipos no existe una póliza de seguros y se incurriría en gastos adicionales.
Conclusión
El Centro de Procesamiento de Datos y los equipos informáticos que no cuentan con una póliza de seguros en caso de suscitarse un desastre o casos fortuitos se perderían los equipos parcial o totalmente y poniendo en riesgo la integridad, confiabilidad y disponibilidad de la información. Además la póliza de seguros es una medida de seguridad física para los equipos informáticos. Finalmente no se cumple con la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.
Recomendación
Se recomienda al Jefe de Gestión Tecnológica implementar en los requerimientos del POA la póliza de seguros, de igual forma al Jefe de Compras públicas implementar en el PAC la póliza de seguros para equipos informáticos.

Elaborado Por:	JCVG	**Fecha:**	16-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Inexistencia de una política para dar de baja los equipos informáticos
Condición
No existe una procedimiento específicos para dar de baja los equipos informáticos obsoletos y son llevados a la bodega
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-04 Políticas y procedimientos señala: La Unidad de Tecnología de la Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.
Causa
No se ha visto necesario implementar una política para dar de baja los equipos informáticos, debido a que se elabora un informe técnico y se entrega mediante actas de entrega/recepción al personal responsable de bodega, quienes se encargan de llevar los equipos a la bodega.
Efecto
Acumulación de equipos obsoletos que no son chatarrizados.
Conclusión
La falta de una política para dar de baja los equipos informáticos produce una inadecuada gestión de los mismos después de haber terminado su vida útil y no se lleva a cabo lo que especifica la Norma Técnica de Control Interno de la CGE, 410-04 Políticas y procedimientos.
Recomendación
Se recomienda al personal de la Unidad de Gestión Tecnológica y al personal de bodega formular y establecer una política para dar de baja los equipos informáticos al haber cumplido su vida útil con el propósito de darle un mejor fin que contribuya al cuidado del medio ambiente y no provocar la acumulación de los mismos.

Elaborado Por:	JCVG	**Fecha:**	17-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Los respaldos de la información no son guardados en algún sitio o ciudad del país
Condición
La institución no utiliza los servicios de empresas con respecto a salvaguardar la información en un lugar externo o en alguna ciudad del país.
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-10 Seguridad de tecnología de información señala: La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ellos se aplicarán las siguientes medidas: Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.
Causa
Escaso presupuesto para contratar servicios de empresas con respecto a salvaguardar la información en lugares externos o incluso ciudades del país.
Efecto
Guardar los respaldos de información en la nube o discos duros no suele ser suficiente para garantizar la integridad y disponibilidad de la información.
Conclusión
La Unidad de Gestión Tecnológica salvaguarda la información mediante el uso de la nube y discos duros, sin embargo para garantizar la disponibilidad e integridad de la misma es necesario contratar los servicios de empresas que guardan la información en sitios externos o ciudades del país.
Recomendación
Se recomienda al Jefe de Gestión Tecnológica implementar en los requerimientos del POA la contratación de servicios de empresas a fin de salvaguardar la información en lugares externos o ciudades del país para garantizar la disponibilidad e integridad de la información institucional.

Elaborado Por:	JCVG	**Fecha:**	17-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

Inutilización de claves fuertes por parte de los funcionarios
Condición
Los funcionarios no poseen contraseñas fuertes de acuerdo a lo que señala el documento formal establecido
Criterio
Según las Normas Técnicas de Control Interno de la CGE, 410-12 Administración de soporte de tecnología de información señala: La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Considerando aspectos como: Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos, temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
Causa
Los funcionarios no utilizan las contraseñas fuertes, de al menos 14 caracteres alfanuméricos, debido a que les toma más tiempo ingresar al computador y al sistema.
Efecto
La inutilización de las contraseñas fuertes que es considerada una medida de seguridad provocaría ataques cibernéticos o incluso puede producir delitos informáticos como el robo de información confidencial.
Conclusión
Los funcionarios no utilizan contraseñas fuertes para encender el computador, tampoco para ingresar al sistema Cabildo ERP para el desarrollo de sus actividades laborales, exponiéndose al robo de información e incumpliendo con la Norma Técnica de Control Interno de la CGE, 410-12 Administración de soporte de tecnología de información.
Recomendación
Se recomienda a los funcionarios del GAD Municipal del Cantón San Pedro de Pelileo utilizar contraseñas fuertes que incluyan al menos 14 caracteres alfanuméricos y caracteres especiales como medida de seguridad para evitar el robo de información confidencial.

Elaborado Por:	JCVG	**Fecha:**	17-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	03-10-2018

NOMBRE DEL INDICADOR	FÓRMULA	UNIDAD DE MEDIDA	FRECUENCIA	CÁLCULO	RESULTADO	ANÁLISIS
Porcentaje de computadoras obsoletas	(Número de computadoras obsoletas en la Institución en el período 2016/Total de computadoras en la Institución en el período 2016)*100	Porcentaje	Anual	(34/134)*100	25.373	El número de computadoras obsoletas representa al 25% las mismas que fueron dadas de baja y almacenadas en la bodega municipal. Con el mantenimiento correctivo respectivo se cambian las piezas defectuosas, sin embargo si no se encuentra solución se reemplaza el equipo.
Porcentaje de Portátiles obsoletas	(Número de portátiles obsoletas en la Institución en el período 2016/Total de portátiles en la Institución en el período 2016)*100	Porcentaje	Anual	(2/17)*100	11.77	El número de portátiles obsoletas representa al 11.77% las mismas que fueron dadas de baja y almacenadas en la bodega municipal.

Elaborado Por:	JCVG	**Fecha:**	20-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	05-10-2018

NOMBRE DEL INDICADOR	FÓRMULA	UNIDAD DE MEDIDA	FRECUENCIA	CÁLCULO	RESULTADO	ANÁLISIS
Porcentaje de Impresoras obsoletas	(Número de impresoras obsoletas en la Institución en el período 2016/Total de impresoras en la Institución en el período 2016)*100	Porcentaje	Anual	(41/107)*100	38.32	El número de impresoras obsoletas representa al 38% las mismas que fueron dadas de baja y almacenadas en la bodega municipal. Para el mantenimiento de las impresoras se requiere contratar un servicio externo debido a la naturaleza del trabajo y reemplazo de partes.
INDICADORES DE EFICACIA						
Soporte Técnico	(Número de asistencias técnicas atendidas en el período 2016/Número de asistencias técnicas solicitadas en el período 2016) *100	Porcentaje	Anual	(1200/1220) *100	98.361	Con respecto al soporte técnico, los técnicos del área de Gestión Tecnológica reciben en promedio 5 llamadas telefónicas a diario, lo que representa 1200 asistencias en el año las mismas que son atendidas en el 98%

Elaborado Por:	JCVG	**Fecha:**	20-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	05-10-2018

NOMBRE DEL INDICADOR	FÓRMULA	UNIDAD DE MEDIDA	FRECUENCIA	CÁLCULO	RESULTADO	ANÁLISIS
Ejecución de proyectos	(Número de proyectos ejecutados en el período 2016/Número de proyectos planificados en el período 2016)*100	Porcentaje	Anual	(6/8)*100	75	De acuerdo al POA 2016 presentado por la Unidad de Gestión Tecnológica se plantearon 8 proyectos de los cuales se cumplieron 6 durante el año, debido a la falta de presupuesto, lo que representa el 75% en ejecución de proyectos ∞
Acceso a Internet	(Número de computadoras que tienen acceso a internet en el período 2016/Total de computadoras en el período 2016)*100	Porcentaje	Anual	(149/159)*100	93.71	Con respecto al acceso a internet, el 93,71% de computadoras tienen acceso a internet, esto se debe a que 10 computadoras que se encuentran en la biblioteca tienen acceso a internet ocasionalmente.

∞ Cotejado con evidencia **H/POA**

Elaborado Por:	JCVG	**Fecha:**	21-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	05-10-2018

INDICADORES PRESUPUESTARIOS						
NOMBRE DEL INDICADOR	**FÓRMULA**	**UNIDAD DE MEDIDA**	**FRECUENCIA**	**CÁLCULO**	**RESULTADO**	**ANÁLISIS**
% de Participación del Presupuesto de la Unidad de Gestión Tecnológica	(Total del presupuesto asignado para la Unidad de Gestión Tecnológica en el período 2016/Total del presupuesto del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	Porcentaje	Anual	($56.749,35/$27'391.396,26)*100	0.21	El porcentaje de participación del presupuesto de la Unidad de Gestión Tecnológica con respecto al total del presupuesto institucional corresponde al 0,21% esto se debe a que dicha Unidad depende de la Dirección Administrativa.

Elaborado Por:	JCVG	**Fecha:**	22-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	05-10-2018

NOMBRE DEL INDICADOR	FÓRMULA	UNIDAD DE MEDIDA	FRECUENCIA	CÁLCULO	RESULTADO	ANÁLISIS
% de Participación del Presupuesto de la Dirección Administrativa	(Total del presupuesto asignado para la Unidad de Gestión Tecnológica en el período 2016/Total del presupuesto asignado para la Dirección Administrativa en el período 2016)*100	Porcentaje	Anual	($56.749,35/$327.711,81) *100	17.32	El porcentaje de participación del presupuesto de la Unidad de Gestión Tecnológica con respecto al presupuesto de la Dirección Administrativa corresponde al 17,32% esto se debe a que dicho programa comprende Unidades como Contratación Pública, Talento Humano, Servicios Generales y Salud Ocupacional.

Elaborado Por:	JCVG	**Fecha:**	22-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	05-10-2018

INDICADORES DE SEGURIDAD						
NOMBRE DEL INDICADOR	**FÓRMULA**	**UNIDAD DE MEDIDA**	**FRECUENCIA**	**CÁLCULO**	**RESULTADO**	**ANÁLISIS**
Seguridad Lógica	(Número de computadoras que cuentan con la contraseña fuerte para ser encendidas en el período 2016/Total de computadoras del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	Porcentaje	Anual	(62/162)*100%	38%	Con respecto a la seguridad lógica apenas el 38% de servidores/as usan una contraseña fuerte para encender el computador.
	(Número de computadoras que cuentan con screensaver o protector de pantalla en el período 2016/Total de computadoras del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	Porcentaje	Anual	(65/162)*100%	38%	Con respecto a la seguridad lógica apenas el 38% de servidores/as usan en sus computadoras el protector de pantalla o screensaver

Elaborado Por:	JCVG	**Fecha:**	23-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	05-10-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Hoja del POA 2016** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI** **H/POA** **1/8**

GOBIERNO MUNICIPAL DE PELILEO

PLAN OPERATIVO ANUAL EJERCICIO ECONÓMICO 2016

DIRECCIÓN: ADMINISTRATIVA

UNIDAD: Gestión Tecnológica

OBJETIVO: Planear, coordinar y supervisar el crecimiento y administración de los Sistemas Integrales y de las Redes de Datos, de Aplicaciones Municipales y sus servicios integrados.

META: Crear una Unidad Tecnológica centralizada y automatizada de información acorde a los métodos y aplicaciones de la Era Actual

ESTRATEGIAS: Gestionar, implementar y difundir el uso de nuevas tecnologías en el trabajo diario e incentivar su aplicación a través de capacitaciones al personal administrativo

PROYECTO	ACTIVIDADES	CRONOGRAMA Cuatrimestre			EQUIPO NECESARIO (Material y Humano)	COSTO (USD)	BENEFICIARIOS	FINANCIAMIENTO	RESPONSABLES	INDICADORES DE GESTIÓN	MEDIOS DE VERIFICACIÓN
		1	2	3							
Mantenimiento de equipos de impresión ∞	Verificar el inventario de software	x	x	x	Servicio técnico especializado	5000	Usuarios y Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Revisión, mantenimiento preventivo y cambio de partes sensibles de las impresoras	Equipos de impresión funcionando correctamente
	Solicitar visto bueno para iniciar el proceso de adquisición										
	Adquirir las licencias a través del Portal de Compras Públicas										
	Activar las licencias adquiridas en los equipos informáticos										
Pago y mantenimiento de la Red WiFi en los parques urbanos ∞	Revisión de los equipos de activos de red	x	x	x	Equipos activos de red, Funcionarios de Tecnología	10000	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Equipos conectados a la red local	Eficiente conexión a la red municipal
	Pruebas de conectividad y respuesta de transmisión de datos										
	Solicitar equipos activos de red de reemplazo en caso de haber averías										
	Instalación y configuración de nuevos equipos activos de red										

∞ **H/I 3/6** Cotejado con indicadores

Elaborado Por:	JCVG	**Fecha:**	24-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	08-10-2018

Soporte al Sistema integral de Gestión Municipal Cabildo ∞	Solicitar autorización y presupuesto al Alcalde Solicitar requerimientos de automatización a las Unidades Municipales Automatizar los requerimientos institucionales Respaldar la información y ejecutar el mantenimiento anual al sistema	x	x	x	Funcionarios de Tecnología y técnicos de PrisHard	6000	Usuarios y Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica, Avalúos, Tesorería, Dir. Financiera, Agua Potable	Sistema funcionando adecuadamente; Unificación de códigos de identificación único transacciones realizadas sin inconvenientes; Reducción de tiempo al realizar los trámites	Sostenibilidad al Software implementado
Adquisición de repuestos y partes informáticas ∞	Diagnóstico de las partes más vulnerables Solicitar la adquisición de acuerdo a los modelos existentes Reposición de los dispositivos dañados	x			Respuestos y Técnico Municipal	3000	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Cambios realizados en equipos que superan en promedio los dos años de funcionamiento	Equipos informáticos operativos
Capacitación en cursos y talleres tecnológicos (ORACLE, PLSQL, SEGURIDAD INFORMÁTICA) ∞	Solicitar autorización para la participación en eventos de capacitación Asistir a cursos y talleres Aplicar los conocimientos en las tareas diarias del trabajo	x	x	x	Personal Municipal	3000	Funcionarios de la municipalidad	Presupuesto Municipal	Jefatura de Gestión Tecnológica	Nuevas técnicas en los procesos informáticos	Personal capacitado en las nuevas tecnologías

Elaborado Por:	JCVG	**Fecha:**	24-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	08-10-2018

Plan de mantenimiento de equipos informáticos ∞	Presentar el Plan Anual de Mantenimiento de equipos informáticos	x	x	x	Herramientas, repuestos, Funcionarios Municipales	2000	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Jefatura de Gestión Tecnológica	Bitácoras con información de los equipos, informes semestrales	Equipos informáticos en buen funcionamiento
	Comunicar el cronograma de mantenimiento a las Unidades Municipales										
	Adquirir herramientas										
	Ejecutar el plan de mantenimiento										
Consulta gráfica de predios en la web ∞	Adquisición de servidor		x		Portal Web, Servidor, Aplicación de consulta	10000	Avalúos y catastros, Ciudadanía en general	Presupuesto Municipal	Unidades de Tecnología y Avalúos y Catastros	Aumentar el espacio de alojamiento y renovar el dominio gubernamental	Portal web de consulta en línea
	Contratación para el desarrollo de la aplicación de consulta										
	Facilitar la información respectiva										
	Acoplar la aplicación al sitio web municipal										
Licencia de firewall ∞	Determinar el tráfico de datos en la red			x	Equipo firewall Funcionarios de la Municipalidad	4000	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Unidad de Tecnología	Equipo adquirido y configurado	Control efectivo de spam y correo no deseado en las páginas web y correos electrónico respectivamente
	Adquirir el modelo de firewall más idóneo										
	Contratar el alojamiento y diseño del sitio										
	Configuración del equipo										

Elaborado Por:	JCVG	**Fecha:**	24-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	08-10-2018

A. RECURSOS DE PERSONAL

GRUPO OCUPACIONAL	Número de Servidores		ASIGNACIÓN ANUAL	Número de Servidores		ASIGNACIÓN ANUAL
	Disponible	RMU		Requerido	RMU	
Directivo			-			-
Profesional			-			-
Técnico	1	817.00	9,804.00			-
Administrativo			-			-
Servidor Público de Apoyo			-			-
Servidor Público de Servicios			-			-
			9,804.00			-
Total RMU LOSEP						9,804.00
Jornadas Ocasionales			-			-
Jornadas Permanentes			-			-
			-			-
Total RMU Código de Trabajo						-
TOTAL GENERAL US$						**9,804.00**√

√ Revisado

Elaborado Por:	JCVG	**Fecha:**	24-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	08-10-2018

B. RECURSOS EN SUMINISTROS Y MATERIALES

CÓDIGO	DETALLE	UNIDAD DE MEDIDA	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0804	**MATERIALES DE OFICINA**				
	Papel bond A4	resma	10	3.50	35.00
	Esferográfico punta gruesa color azul	u	20	0.80	16.00
	Frasco de tinta negro EPSON	u	5	10.00	50.00
	Frasco de tinta amarillo EPSON	u	2	10.00	20.00
	Frasco de tinta azul EPSON	u	2	10.00	20.00
	Frasco de tinta rojo EPSON	u	2	10.00	20.00
	Lapiceros	u	5	4.00	20.00
	Archivador tamaño oficio	u	10	3.50	35.00
	Resaltador varios colores fosforecentes	u	3	1.20	3.60
	Tijera pequeña	u	1	1.50	1.50
	Portapapeles de 3 pisos	u	3	10.00	30.00
	Memory flash 16 GB	u	3	20.00	60.00
	Torre de 100 CD IMATION	u	1	50.00	50.00
	Torre de 100 DVD IMATION	u	1	80.00	80.00
	Subtotal US$				**441.10** √

Elaborado Por:	JCVG	**Fecha:**	24-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	08-10-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Hoja del POA 2016** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI H/POA 6/8**

CÓDIGO	DETALLE	UNIDAD DE MEDIDA	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0805	**MATERIALES DE ASEO**				
	Franela	metro	3	2.00	6.00
	Guaipe	funda	3	5.00	15.00
	Jabón líquido	galón	1	15.00	15.00
	Escoba y pala con mango	u	1	15.00	15.00
	Basurero metálico	u	1	20.00	20.00
	Subtotal US$				**71.00** √
0806	**HERRAMIENTAS**	u	1		
	Juego de llaves	u	1	80.00	80.00
	Juego de desarmadores planos	u	1	80.00	80.00
	Alicate	u	1	20.00	20.00
	Juego de desarmadores estrellas	u	1	80.00	80.00
	Juego de desarmadores hexagonales	u	1	80.00	80.00
	Taladro	u	1	80.00	80.00
	Subtotal US$				**420.00** √
0809	**MEDICAMENTOS**				-
	Subtotal US$				-
0811	**MATERIALES DE CONSTRUCCIÓN, ELÉCTRICOS, PLOMERÍA, CARPINTERÍA**				-
	Subtotal US$				-

Elaborado Por:	JCVG	**Fecha:**	24-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	08-10-2018

CÓDIGO	DETALLE	UNIDAD DE MEDIDA	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0813	**REPUESTOS Y ACCESORIOS**				
	Fuente de poder 600 WATTS	u	10	30.00	300.00
	Disco duro SATA 500 GB	u	5	120.00	600.00
	Regulado de voltaje	u	5	20.00	100.00
	Teclado USB	u	10	15.00	150.00
	Rollo de Cable UTP 5e	u	1	100.00	100.00
	Conectores RJ45	u	100	0.30	30.00
	Mouse USB	u	10	10.00	100.00
	Subtotal US$				**1,380.00**√
0819	**ACCESORIOS E INSUMOS QUIMICOS Y ORGÁNICOS**				-
	Subtotal US$				-
				TOTAL US$	**2,312.10**√

√ **Revisado**

Elaborado Por:	JCVG	**Fecha:**	24-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	08-10-2018

GASTOS EN INFORMÁTICA

CÓDIGO	DETALLE	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0701	**DESARROLLO, ACTUALIZACIÓN, ASISTENCIA TÉCNICA Y SOPORTE DE SISTEMAS INFORMÁTICOS**			
	Asistencia técnica sistema CABILDO	1	6,000.00	6,000.00
	Subtotal US$			**6,000.00**
0702	**ARRENDAMIENTOS Y LICENCIAS DE USO DE PAQUETES INFORMÁTICOS**			
	Renovación licencia Firewall	1	4,000.00	4,000.00
	Pago de internet en zonas Wifi Urbanos	3	2,500.00	7,500.00
	Subtotal US$			**11,500.00**
0703	**MANTENIMIENTO Y REPARACIÓN DE EQUIPOS Y SISTEMAS INFORMÁTICOS**			
	Mantenimiento impresoras del GAD	95	50.00	4,750.00
	Mantenimiento generador eléctrico	2	500.00	1,000.00
	Mantenimiento de zonas Wifi Urbanos	1	2,500.00	2,500.00
	Mantenimiento aire acondicionado	1	150.00	150.00
	Subtotal US$			**8,400.00** √
			TOTAL US$	**25,900.00** √

√ **Revisado**

Elaborado Por:	JCVG	**Fecha:**	24-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	08-10-2018

FACTORES DE RIESGO	
Impredecibles Inciertos	**Desastres Naturales:** Incendios, lluvias, humedad, calor, ceniza.
	Tecnológico: Ataque de virus informáticos (Amenazas Lógicas),malware o programas maliciosos, cortos circuitos, fallas de software y hardware
Predecibles	**Humanos:** hacker, cracker, robos, fraude y delito informático, desinstalación de programas bases y/o instalación de programas que impidan el normal funcionamiento del computador

INTERPRETACIÓN:

La Unidad de Gestión Tecnológica está expuesta a riesgos impredecibles como incendios, lluvias (puede ocasionar filtros de agua en el techo donde se encuentra ubicada la unidad y los equipos informáticos); se recomienda colocar los equipos en un lugar donde no sean afectados por las malas condiciones climáticas.

Además la información institucional se encuentra expuesta a riesgos tecnológicos como ataques informáticos y virus informáticos para lo cual se recomienda realizar los respectivos controles a fin de salvaguardar la información.

Finalmente se determinó que el riesgo predecible humano al que se encuentra vulnerable el área, es el fraude y sabotaje por lo que se recomienda la instalación de cámaras de seguridad.

Elaborado Por:	JCVG	**Fecha:**	27-08-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	17-10-2018

ADMINISTRACIÓN GENERAL														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN AUDITORÍA
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
1								TOSHIBA P55-B5206SL	S9E049914S			CAIZABANDA MANUEL	ALCALDIA	∈
2	HP PRO 6300	MXL3200797	HP	LV1911	6CM3101NWP	EPSON L655	W8AY006710					GUEVARA TINTIN GLADYS PATRICIA	ARCHIVO	∈
3	HP 400 G3 SFF	MXL7011CYT	HP	V194	3CQ6251NX3	EPSON L655	W8AY006713					PAREDES ALDAS JAIRO LEVI	COMUNICACION INSTITUCIONAL	∈
4	HP 600 G2 SFF	MXL61016WF	HP	HP V193	3CQ5311HH9							MALUSIN DORYS	CONCEJO MUNICIPAL	∈
5	HP PRO 6200	MXL22710BH	LG	LG L1753T	702NDWE5U561	EPSON L575	W98Y003341					MALUSIN DORYS	CONCEJO MUNICIPAL	∈
6	HP 600 G2 SFF	MXL61016VY	SAMSUNG	733NW	CM17H9FS519687P	HP LASERJET	CNB8D22VNF	DELL INSPIRON	71B1GR1	HP SCANJET PRO 2500	CN74MA10DW	BOURGEAT FLORES PEPITA XIMENA	SECRETARIA GENERAL	∈
7	HP 400 G1 MT	MXL43720RL	HP	LV1911	6CM4271RQQ	EPSON L555	S4VY023368					MAROTO AYALA CATALINA DEL ROCIO	SECRETARIA GENERAL	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO ADMINISTRATIVO														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
8						HP PHOTOSMART PLUS V210	CN0842G2BC	TOSHIBA SATELLITE S55-A5279	XD193327S			LLUGLLA ZUÑIGA JOSE STALIN	COMPRAS PÚBLICAS	∈
9						EPSON L575	W98Y003550							∈
10						EPSON L555	S4VY049496	TOSHIBA SATÉLITE S55-A5279	XD223872S			RAMOS JESSICA	COMPRAS PÚBLICAS	∈
11	HP PRO 6200	MXL12510JP	HP	S2032	CN41130KKZ	EPSON L6171	X4ER000730					BARRERA MARIA ISABEL	DIRECCION ADMINISTRATIVA	∈
12	HP 400 G1 MT	MXL4371Z59	BEN-Q	BENQ G925HDA	ETT3B02692019	EPSON L375	WGBK195574					CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITOR
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
13	HP PRO 6300	MXL3450YKS	HP	HP LV1911	6CM3101QVC			TOSHIBA SATELLITE S55-A5279	XD193533S			CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	∈
14	HP PRO 6300	MXL320078V	HP	HP W1907	3CQ8161V30	EPSON L655	W8AY006719	HP ELITE BOOK 8440P	CND0490M4G			FLORES MAZON JULIO ADALBERTO	GESTION TECNOLOGICA	∈
15	HP 400 G1 MT	MXL4371Z24	HP	HP LA2405x	CN43301NNP	EPSON L350	Q8BK004945			Escaner Xerox DocuMate 3115	3BEEH40084	GUATO GUEVARA MIGUEL ANGEL	GESTION TECNOLOGICA	∈
16	HP ELITE DESK 800 G1	MXL5362PKT	HP	HP V193	3CQ43935MS	EPSON L565	VJDY050507					MIRANDA SELENE	MEDICINA OCUPACIONAL	∈
17	HP PRO 3130 MT	MXL11803YZ	HP	S2032	CN40490KHM	EPSON L555	S4VY157577					GUTIERRES PATRICIA	TALENTO HUMANO	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
18	HP PRO 6300	MXL320078J	HP	LV1911	6CM21510P5	EPSON L555	S4VY023374					MORALES SILVIA	TALENTO HUMANO	∈
19	CLON INTEL CORE 2DUO	SN	LG	W1943C	001NDVWAC703							TUBON ALDAZ FRANKLIN DANIEL	TALENTO HUMANO	∈
20	HP 400 G4 SFF	MXL722151J	HP	V194	3CQ7201RKM	EPSON L555	S4VY023374					TUBON ALDAZ FRANKLIN DANIEL	TALENTO HUMANO	∈
21	HP 400G1 MT	MXL4412YMB	HP	LV1911	6CM4271SPG	EPSON L555	S4VY157588					PERRAZO JUAN CARLOS	RIESGOS LABORALES	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO DE AGUA POTABLE Y ALCANTARILLADO

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
22	HP 400G1 MT	MXL4371Z6G	HP	LV1911	6CM4271SFC	EPSON L655	W8AY007705	SONY VAIO VPCCW21FX	275067848020325			GAMBOA ESCOBAR WILSON RAFAEL	AGUA POTABLE	∈
23			HP	LV911	6CM4271SBT	EPSON L555	S4VY147224							∈
24	HP PRO 6300	MXL3450YJL	HP	L1706	CNN54428LV							PADRON KLEBER	AGUA POTABLE	∈
25	HP PRODESK 400 G4	MXL8170YZZ											AGUA POTABLE	∈
26	HP 400 G4 SFF	MXL7221ZCZ	HP	V194	3CQ7201RJC							SANCHEZ CARLOS	AGUA POTABLE	∈
27	HP PRO 6300	MXL3200796	HP	LV1911	6CM3101N7W	EPSON FX890	E8BY168021					VILLARROEL CHAVEZ MARLON IVAN	AGUA POTABLE	∈
28	HP 400 G3 SFF	MXL7011CX7	HP	V194	3CQ6251NX0							COVA CAROLINA	LABORATORIO	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

ASESORÍA JURÍDICA														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITO
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
29	HP 400 G3 SFF	MXL7011CRV	HP	V194	3CQ6251NWV							PILLA MARIA ELENA	ASESORIA JURIDICA	∈
30	HP PRO 6300	MXL3040BTK	HP	LV1911	6CM2421C39							MORALES GÓMEZ DELIA MARIBEL	ASESORIA JURIDICA	∈
31	HP PRO 6200	MXL13704RO	HP	LV1911	CNK11404QCT	EPSON L555	S4VY023367					RODRIGUES CAROLINA	ASESORIA JURIDICA	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

AUDITORÍA INTERNA														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
32	HP PRO 400 G1 MT	MXL4420X49	HP	LV1911	6CM1271RQV	EPSON L555	S4VY147222	TOSHIBA P55-B5206SL	9E056176S	HP SCANJET PRO 2500	CN7AQA10HS	GRANIIZO MARCO	AUDITORIA INTERNA	∈
33						EPSON L656	W8BY003295							∈
34	CLON INTEL CORE 2DUO	SN	SAMSUNG	733 NW	CM17H9FS518958E	SAMSUNG ML1865	Z5NIBAAB600684F					MASAQUIZA ALEXANDRA	AUDITORIA INTERNA	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	27-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

AVALUOS Y CATASTROS														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
35	HP PRO 6300	MXL320077Y	HP	LV1911	6CM3101N71							AILLON CARRASCO ALBA DE LOURDES	CATASTROS y AVALUOS	∈
36	HP ELITE DESK 800 G1	MXL60219C3	HP	222va	CNK6110BTL			HP PROBOOK 6470b	CNU31392YG			GUZMAN MANUEL	CATASTROS y AVALUOS	∈
37	HP PRO 6200	MXL13824MH	HP	LV1911	6CM3101NVS									∈
38	HP PRO 6300	MXL320077X	HP	S2032	CN41130TB5									∈
39			HP	S2032	CN41140NP1									∈
40			HP	LV1911	6CM4271SB3									∈
41						EPSON L6171	X4ER000643							∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	28-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
42	HP 400 G1 MT	MXL4412YMF	HP	LV1911	6CM4271SBV	HP 9800	MY5C31Z0HJ					VILLALBA WILIAN	CATASTROS y AVALUOS	∈
43	HP PRO 6300	MXL3200793	HP	LV1911	6CM3101NTX	EPSON L200	PRFK076331					MORALES CARGUA ALFREDO ALBERTO	CATASTROS y AVALUOS	∈
44	HP 400 G1 MT	MXL4413LRL	HP	LV1911	6CM4271SC5	HP K8600	TH8AA220FZ					MURGUEITIO RECALDE PABLO RODRIGO	CATASTROS y AVALUOS	∈
45	HP 400 G1 MT	MXL43720SN	HP	LV1911	6CM4271SBD	EPSON FX 890	E8BY024435					PILLA CUNALATA SEGUNDO EDUARDO	CATASTROS y AVALUOS	∈
46	HP 400 G1 MT	MXL4420X4C	LG	22MP48HQP	801NTMX3T971	EPSON L555	S4VY157584					VARGAS CURIPALLO JAVIER ROLANDO	CATASTROS y AVALUOS	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	28-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
47	HP PRO 6300	MXL3450YNS	LG	22MP48HQP	801NTEP3T972							VITERI LUIS ALBERTO	CATASTROS y AVALUOS	∈
48	HP PRODESK 400 G4	MXL8170YZQ	LG	22MP48HQP	801NTVT3T986							MAZON CUEVA ANTONIO	CATASTROS y AVALUOS	∈
49	HP PRODESK 400 G4	MXL8170ZOL	LG	22MP48HQP	801MTBK3T981	HP LASERJET PRO 400	PHGFD38742					AILLON CARRASCO ALBA DE LOURDES	CATASTROS y AVALUOS	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	28-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DESARROLLO DE LA COMUNIDAD														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
50	CLON INTEL CORE 2DUO					HP 1018	CNB1638916					RODRIGUEZ NATALIA	BIBLIOTECA	∈
51	HP PRODESK 400 G4	MXL8170ZOG	LG	20MP38HQB	609NTLE3P864	EPSON L6171	X4ER000930							∈
52						SAMSUNG ML2010	4461BKAP808709							∈
53	HP PRO 6300	MXL13704H6	HP	HP S2032	CN412205HB	EPSON L655	W8AY005556					CAIZABANDA DOLORES	JUNTA DERECHOS	∈
54	HP PRO 6300	MXL13704TY	HP	HP S2032	CN41150RNK									∈
55	HP PRO 6300	MXL1412Q5J	HP	HP S2032	CN412205DD									∈
56	HP PRO 6200	MXL2270QDJ	HP	HP LV1911	6CM21510PJ			HP PROBOOK 6360b	2CE2351X5F			AGUAGUIÑA SANCHEZ MARIA ISOLINA	CULTURA	∈

∈ Verificación física

Elaborado Por:	JCVG	**Fecha:**	29-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
57	HP 400 G1 MT	MXL4413L3C	HP	LV1911	6CM4271SB6	EPSON L555	S4VY147223					RODRIGUEZ EDISON	DEPORTES	∈
58	CLON		LG	L1718S	706UXGL00415	EPSON L555	S4VY147217							∈
59	HP PRO 6200	XML14005Q0	HP	LV1911	6CM3101QTX	EPSON L200	PRFK163484					WILFRIDO SANCHEZ	DESARROLLO COMUNIDAD	∈
60						HP LASERJET 1200	CNBJG13660							∈
61						EPSON L6171	X4ER000924					PICO FERNANDO	DESARROLLO COMUNIDAD	∈
62	HP PRO 400 G1 MT	MXL4413L54	HP	LV1911	6CM4271S9R	EPSON L555	S4VY147218							∈
63	HP dc5700	MXJ738049W	HP	HP1706	CNC735PB6B							VELASTEGUI NAPO	ECONOMIA POPULAR Y SOLIDARIA	∈
64	CLON	SN	SAMSUNG	733NW	CM17H9FS51969OM	EPSON L655	W8AY006878							∈
65	HP PRODESK 400 G4	MXL8170ZOP	LG	20MP38HQB	804NTHM9H585									∈

∈ **Verificación física**

Elaborado Por:	JCVG	Fecha:	29-08-2018

Revisado Por:	WGYCH/CVBP	Fecha:	30-11-2018

FÉNIX IVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Inventario de Hardware** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI** **I/HW** **13/32**

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
66	HP 400 G1 MT	MXL4371YZ0	HP	LV1911	6CM4271RLW	EPSON L555	S4VY157578					TORRES NUÑEZ DORYS ELIANA	PSICOLGIA	∈
67	HP 400 G4 SFF	MXL7221ZBY	HP	V194	3CQ7201RKP	EPSON L350	Q8BK008787					MAYORGA MORALES ENRIQUE ROMEO	TURISMO	∈
68	HP PRODESK 400 G4	MXL8170YZW	LG	20MP38HQB	804NTAB9H864	EPSON L						VILLAGOMEZ MAURICIO	TRABAJO SOCIAL	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	29-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO FINANCIERO														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
69	HP 400 G1 MT	MXL4371Z72	HP	LV1911	6CM4271SBS	EPSON L655	W8AY006703					MORALES CANDO FERNANDO SANTIAGO	ACTIVOS	∈
70	HP PRO 6300	MXL320078P	HP	LV1911	6CM3101QVG	EPSON L555	SAVY147221					VILLACIS NESTOR	ACTIVOS	∈
71	HP PRODESK 400 G4	MXL8170YZW	LG	20MP38HQB	804NTAB9H600	EPSON L655	W8AY006709					GALLEGOS ROTMAN	COACTIVAS	∈
72								DELL INSPIRON N4050	2Z91GR1			PAZ SANCHEZ ELVIA XIMENA	CONTABILIDAD	∈
73	HP PRO 6300	MXL3211QJ4	HP	LV1911	6CM3060LTW	HP LASERJET 1320	CNHC63916F	TOSHIBA P55-B5206SL	9E056133S			ALTAMIRANO BLANCA	DIRECCION FINANCIERA	∈
74						EPSON L6171	X4ER000907							∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	29-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
75	HP 400 G3 SFF	MXL7011CSB	HP	V194	3CQ6251NXB	HP LASERJET PRO 400	CNB8D40S2B					PICO NAVARRETE VERONICA ELIZABETH	DIRECCION FINANCIERA	∈
76	HP PRO 6300	MXL3040BV0	HP	HP LV1911	6CM2421FSB	HP LASERJET CM3530FS	CNJLB02144					VILLARROEL LLERENA YAJAIRA MARIBEL	PRESUPUESTO	∈
77	HP PRO 6200	MXL13704QQ	HP	LV1911	CNK11404XLT	EPSON L200	PRFK040765					BENITEZ FERNANDA	RENTAS	∈
78	CLON INTEL CORE 2DUO	SN	LG	W1943C	001NDFVAC699	EPSON L6171	X4ER000924					MURGUEITIO RECALDE BERTHA MARIANELA	RENTAS	∈
79	HP PRO 400 G1 MT	MXL4371Z2D	HP	LV1911	6CM4271SPL	EPSON FX2190	FCTY080725							∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	30-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

FÉNIX IVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Inventario de Hardware** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI** **I/HW** **16/32**

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGUN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
80	HP PRO 6200	MXL1240KW9	HP	HP S2032	CN41140MLJ			DELL I7 6500	3LP8RF2			GALLEGOS PICO MIRIAM DE LOURDES	TESORERIA	∈
81	HP PRO 6200	MXL2270QJG	HP	HP LV1911	6CM21510PW									∈
82	CLON	SN	HP	LV911	6CM301QW2									∈
83	HP PRO 6200	MXL2270QHW	LG	LG FLATRON L177WSB	806NDZJ8D949	SAMSUNG ML2010	4461BKBQ121062B					PILLA ELENA	TESORERIA	∈
84	HP PRO 6200	MXL2231X2C	HP	L1710	CND80306BL	EPSON FX890	NZBY072326					MAZON MEZA JUAN CARLOS	VENTANILLA 1	∈
85			LG	20MP38HQB	804NTMX9H859	HP LASERJET PRO 400	PHGFD38739							∈

∈ Verificación física

Elaborado Por:	JCVG	**Fecha:**	30-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN AUDITORÍA
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
86	HP PRO 6201	MXL22710B0				EPSON FX890	NZBY072306					PAREDES ANITA	VENTANILLA 2	∈
87			LG	20MP38HQB	804NTMX9H588	HP LASERJET PRO 400	PHGFD39208							∈
88	HP PRO 6200	MXL2270QFV	SAMSUNG	740N	HA17H9NP804353EMI	EPSON FX890	NZBY003600					CESPEDES GAVILANES CECILIA ISABEL	VENTANILLA 3	∈
89			LG	20MP38HQB	804NTMX9H584	HP LASERJET PRO 400	PHGFD39180							∈
90	HP PRO 6200	MXL2270QGL	HP	LV911	6CM21510P3	HP LASERJET PRO 400	PHGFD39203					VILLARROEL MARIO	VENTANILLA 4	∈
91			LG	20MP38HQB	804NTMX9H860	EPSON FX890	NZBY003597							∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	30-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

ADMINISTRACIÓN DE JUSTICIA															
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
92	HP 600 G2	MXL61016W5	HP	V194	3CQ53111HL5	EPSON L575	W98Y003340					VERA JORGE LUIS	COMISARIA MUNICIPAL	∈
93	HP PRO 6200	MXL13704RP	HP	LE1911	CNK11404XH	EPSON FX890	NE8BY076882							∈
94	HP 400 G4 SFF	MXL7221ZCL	HP	V193	3CQ7201RKQ									∈
95	HP 400 G4 SFF	MXL7221ZC3	HP	V194	3CQ7201RK5	SAMSUNG ML2010	4461BKBQ121040A					RIVERA OSCAR	JUSTICIA	∈
96	HP 400 G4 SFF	MXL722151W	HP	V194	3CQ7201RK9	EPSON L655	W8AY006711					VILLENA DIANA	JUSTICIA	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	30-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO DE OBRAS PÚBLICAS														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN AUDITORÍA
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
97	HP 400 G4 SFF	MXL7221ZCJ	SAMSUNG	2233SN	CM22H9LS413194V	SAMSUNG ML2010	4461BKDP719772J					AILLON CARRASCO ROBERTO EDISON	OBRAS PUBLICAS	∈
98	CLON INTEL CORE 2DUO	SN	LG	W1943C	005NDMT5M163									∈
99	CLON INTEL CORE 2DUO	SN	HP	LV1911	6CM3101QV9									∈
100	HP PRO 6300	MXL3200780	HP	LV1911	6CM3101NV5	HP 9800	MY5CN1Z14G							∈
101	HP PRO 6300	MXL3200799	SAMSUNG	2233SN	CM22H9LS413817Y							MARCELO ACUÑA	OBRAS PUBLICAS	∈
102	CLON INTEL CORE 2DUO	SN	LG	W1943C-PF	001NDVWAC679							MASAQUIZA WILIAN	OBRAS PUBLICAS	∈
103	HP PRODESK 400 G4	MXL8170YZX												∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
104	CLON INTEL CORE 2DUO	SN	HP	LV1911	6CM4271SB9	HP LASERJET 1200	CNBJK20094					RIOFRIO GEOVANY	OBRAS PUBLICAS	∈
105						EPSON C351C	LD9Y014684							∈
106	HP PRO 6300	MXL320079F	HP	LV1911	6CM3101N77	EPSON L555	S4VY023962					VILLENA MACHADO LUIS EDUARDO	OBRAS PUBLICAS	∈
DEPARTAMENTO DE ORDEN Y CONTROL														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
107	HP PRO 6300	MXL3441CMG	HP	LA2405x	CN43301NZ3							CUNALATA FABIANA	ORDEN Y CONTROL	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
108	HP PRO 6300	MXL3040BW2	HP	LV1911	6CM2421DYR	EPSON L555	S4VY023366					FREIRE GRACIELA	ORDEN Y CONTROL	∈
109	HP 400 G4 SFF	MXL7221ZCS	HP	V194	3CQ7201RKX							JEREZ MAGALI	ORDEN Y CONTROL	∈
110	HP PAVILION S3220la	CNIA735062S	SAMSUNG	740N	HA17H9NLA19608W	EPSON L200	PRFK040761					LLERENA EDUARDO	ORDEN Y CONTROL	∈
111	HP PRODESK 400 G4	MXL8170ZOJ	LG	20MP38HQB	604ERSW02934									∈
112	HP PRO 6200	MXL125038C	HP	LE1911	CNK1140768	EPSON L655	W8AY005555	HP PROBOOK 6470b	CNU31392YL			PAREDES MARIELA	ORDEN Y CONTROL	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO DE PLANIFICACIÓN

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
113	HP PRO 6200	MXL13824MY	SAMSUNG	2233SN	CM22H9LS413209X							ALDAS JESSICA	PLANIFICACION	∈
114	HP PRO 6300	MXL320078G	HP	V193	3CQ4472M2G							BARONA KLEVER	PLANIFICACION	∈
115	HP PRO 6300	MXL3441CMF	HP	LV1911	6CM3101QW6							GUAYPATIN SANCHEZ MIRIAN MARGOT	PLANIFICACION	∈
116	CLON INTEL CORE 2DUO	SN	HP	LV1911	6CM3101N8F							HERNANDEZ ANDRES	PLANIFICACION	∈
117	HP PRODESK 400 G4	MXL8170YZR												∈
118	CLON INTEL CORE 2DUO	SN	HP	LV1911	6CM3101N7G							MAROTO DANNIEL	PLANIFICACION	∈
119	HP PRODESK 400 G4	MXL8170Z05												∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

FÉNIX IVG AUDITORES & CONSULTORES ASOCIADOS	**GAD Municipal del Cantón San Pedro de Pelileo** **FASE II: EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA: Inventario de Hardware** **Del 1 de Enero al 31 de Diciembre del 2016**	**EAI** **I/HW** **23/32**

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	ESTADO SEGÚN
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
120	HP PRO 6300	MXL320079B	LG	FLATRON L1752TX-SF	606NTVS2T759							MAYORGA FABIAN	PLANIFICACION	∈
121	CLON INTEL PENTIUM IV	SN	HP	LV1911	6CM3101NV4									∈
122	HP PRO 6300	MXL320078Z	HP	LA2405x	CN43301NPB			SONY VAIO VPCCW21FX	275067343019982			MORALES ERNESTO	PLANIFICACION	∈
123	HP PRO 6300	MXL3441CMN	HP	LA2405x	CN43301NPY	HP LASERJET 1022	CNBC5DL154					PUNINA RECALDE FREDY RAUL	PLANIFICACION	∈
124	HP PRO 6300	MXL3200790	SAMSUNG	2233SN	CM22H9LS413202B							TORRES RAUL	PLANIFICACION	∈
125	HP 400 G1 MT	MXL4371YXL	HP	LA2405x	CN43301NQJ	SAMSUNG ML2010	4461BKDP727400D					YANZAPANTA JHON LEONARDO	PLANIFICACION	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

REGISTRO DE LA PROPIEDAD														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
126	HP 400 G1 MT	MXL4371YZ4	HP	HP S2032	CN41130T70	HP PHOTOSMART PLUS V210	CN15EF441T					ALVARADO MIGUEL	REGISTRO DE LA PROPIEDAD	∈
127						EPSON FX890	NZBY018375							∈
128	HP PRO 6200	MXL14005Q5	HP	HP S2032	CN41161CNV	EPSON FX890	NZBY095487					GUATO DIANA	REGISTRO DE LA PROPIEDAD	∈
129	HP PRO 6200	MXL13824MB	HP	HP S2032	CN41140NNC	HP 4500	CN15EF4403					MORALES MEDARDO	REGISTRO DE LA PROPIEDAD	∈
130						EPSON FX890	NZBY095490					MORALES MEDARDO	REGISTRO DE LA PROPIEDAD	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
131	HP PRO 6200	MXL14005SJ	HP	HP S2032	CN41140LJS	HP 4500	CN15EF23H6					MORALES PERRAZO CARLOS ALBERTO	REGISTRO DE LA PROPIEDAD	∈
132						EPSON FX890	NZBY095507							∈
133	HP 400 G1 MT	MXL4371Z16	HP	HP S2032	6CM4271SC8	HP LASERJET 1200	CNB8D4LVFX							∈
134	HP PRO 6200	MXL14005PQ	HP	HP LV1911	6CM4271SCB	EPSON L6171	X4ER000925							∈
135	HP PRO 6200	MXL14005PV	HP	HP S2032	CN41140NHK	EPSON FX890	NZBY018693					RIOFRIO ERNESTO	REGISTRO DE LA PROPIEDAD	∈

∈ Verificación física

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

DEPARTAMENTO DE SERVICIOS PÚBLICOS														
N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
136	HP 400 G1 MT	MXL4420X2Z	HP	LV1911	6CM4271RQ5							CEVALLOS CARMEN	CAMAL MUNICIPAL	∈
137	HP PRO 6300	MXL3040BVJ	HP		6CM2421H7R	HP LASERJET PRO 400	PHGFD38726					PAREDES VERONICA	CAMAL MUNICIPAL	∈
138	HP PRO DESK 400 G4	MXL8170YZP	LG	20MP38HQB	804NTWG9H601	EPSON L6171	X4ER000937					LASCANO ROSA OBDULIA	CAMAL MUNICIPAL	∈
139	HP PRO 6300	MXL3441CNG	HP	LA2405X	CN43301NNM	SAMSUNG ML2010	BKB31606P	HP PAVILION DX6-7000	2CE2430PNY			LLERENA NUÑEZ WILSON BLADIMIR	GESTION DE RIESGOS	∈

∈ Verificación física

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGUN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
140	HP PRO 400 G1 MT	MXL4413L5N	HP	HP LV1911	6CM4271RLN	EPSON L555	S4VY023371					GALLEGOS MAZON FABIAN MANUEL	MERCADO REPUBLICA DE ARGENTINA	∈
141	HP PRO 6300	MXL320078T	HP	HP V193	3CQ4472MP4	EPSON L								∈
142	CLON INTEL CORE 2DUO	SN	HP	LV1911	6CM3101QTX	EPSON L6171	X4ER000926							∈
143	HP ELITE DESK 800 G1	MXL54510BR	HP	HP V193	3CQ4472MP4	HP LASERJET PRO 400	PHGFD38731					MALUCIN VERONICA	MERCADO REPUBLICA DE ARGENTINA	∈
144	CLON INTEL CORE 2DUO	SN	SAMSUNG	733NW	CM17H9FS518840X	EPSON L555	S4VY023365	LAPTOP HP DV4-1120US	3C8421PF5			VILLARROEL CHAVEZ CESAR AUGUSTO	PLAZAS Y MERCADOS	∈
145	CLON INTEL CORE 2DUO	SN	LG	L1752TQ	606NTKF2T557	EPSON LX-300+	CDUY112706							∈
146	HP PRODESK 400 G4	MXL8170YZS				SAMSUNG ML1740	BKCY114987A							∈

∈ **Verificación física**

Elaborado Por:	JCVG	Fecha:	31-08-2018

Revisado Por:	WGYCH/CVBP	Fecha:	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITOR
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
147	HP PRO 6200	MXL1240L07	HP	HP LV1911	6CM3101QVN							GALLEGOS BALSECA DIPSON	POLICIA MUNICIPAL	∈
148	HP PRO 6300	MXL320078Y	HP	HP S2032	CN41130KL4	EPSON L555	S4VY049505							∈
149	HP PRO 6300	MXL320079D	HP	LV1911	6CM3101N7K	HP LASERJET 1200	CNBJM21745					LLERENA NUÑEZ EDUARDO	SEGURIDAD CIUDADANA	∈
150						HP LASERJET 1200	CNC3106105							∈
151						EPSON TX730WD	N96Y003091					LLERENA NUÑEZ WILSON BLADIMIR	RIESGOS	∈

∈ Verificación física

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
152	CLON INTEL CORE I3	LMA100008	HP	L1706	CNC741P1D7	HP 9800	MY5C01Z0G9					NUÑEZ IVAN	SEGURIDAD Y RIESGOS	∈
153	HP PRO DESK 400 G4	MXL8170YZW												∈
154	CLON INTEL CORE 2DUO	SN	LG	W1943C	910NBAYTM008							OCHOA LUCIA	SERVICIOS PUBLICOS	∈
155	HP 400 G4 SFF	MXL7221ZCH	HP	V194	3CQ7201RBF	HP LASERJET CM2320N	CND999J022					OÑA DANIEL	SERVICIOS PUBLICOS	∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

N°	COMPUTADOR ESCRITORIO		MONITOR			EQUIPO DE IMPRESION		COMPUTADOR PORTATIL		OTROS DISPOSITIVOS		CUSTODIO	DEPENDENCIA	SEGÚN AUDITORÍ
	MODELO	SERIE	MARCA	MODELO	SERIE	MARCA	SERIE	MARCA MODELO	SERIE	MARCA MODELO	SERIE			
156	HP PRO 6300	MXL3040BTV	HP	LV1911	6CM2421BL9	LEXMARK						URQUIZO CARLOS IBAN	COMPLEJO LA MOYA	∈
157	CLON INTEL CORE 2DUO	22U15E2018F1509	LG	L177WSB	802NDSK6A278	EPSON L350	Q8BK003817							∈
158	HP PRODESK 400 G4	MXL8170YZW				EPSON L6171	X4ER000905							∈

∈ **Verificación física**

Elaborado Por:	JCVG	**Fecha:**	31-08-2018

Revisado Por:	**WGYCH/CVBP**	**Fecha:**	30-11-2018

SERVIDORES

USUARIO/CUSTODIO	DEPENDENCIA	DESCRIPCION		N° SERIE	PROCESADOR	RAM	DISCOS DUROS		SISTEMA OPRATIVO	SERVICIOS
		Marca/Modelo	GENERACIÓN				CAPACIDAD	TIPO		
LLERENA NUÑEZ WILSON BLADIMIR	GESTION DE RIESGOS	SERVIDOR		FZUP1141360		16 GB	5 X 2 TB	SATA	CENTOS	
MORALES PERRAZO CARLOS	REGISTRO DE LA PROPIEDAD	HP PROLIANT ML 350p	8	2M22510148					WINDOWS SERVER 2008 R2	Sistema Registral
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT ML370	6	MXQ14700N3	XEON E5645 2,4GHz	16 GB	2x500 GB	SAS	WINDOWS SERVER 2008 R2	Reloj Biometrico, Consola Antivirus
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT ML370	5	USEC821N817	XEON E5430 2,6GHz	4 GB	3x146 GB	SAS	WINDOWS SERVER 2003 R2	Sigame
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP ML110		MX282000DC					CENTOS 6,5	Servidor Internet
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT ML370	4	BRC610N0LA			3X72,8 GB	SCSI		
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT ML 350p	8	2M230701HP			2X1 TB	SATA	CENTOS 6,5	Pruebas Cabildo
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT DL 360	9	MXQ54008M8	2 x XEON E2630 2,6GHz	2 x 16 GB	2 x 2TB	SAS	CENTOS 6,5	Cabildo Alfanumérico y Grafico
CARRASCO PERRAZO LUIS GUILLERMO	GESTION TECNOLOGICA	HP PROLIANT DL 160	6	MXQ93206XW					CENTOS 6,5	Consultas Web

Elaborado Por:	JCVG	**Fecha:**	31-08-2018	**Revisado Por:**	**WGYCH/CVBP**	**Fecha:**	30-11-2018

EQUIPOS DE RED

UBICACIÓN	EQUIPO	MARCA/MODELO	SERIE
DESARROLLO DE LA COMUNIDAD	CENTRAL IP	GRANDSTREAM UCM 6202	21AWMJMG709A5987
	SWITCH	HP 1420 (24 PUERTOS POE+ 12 PUERTOS)	CN57GVK0FT
	ROUTER	MIKROTIK RB951UI-2HND	6BF407050950
DATA CENTER	SWITCH 54p capa3	CISCO SG300-52P	PSZ21281ACX
	SWITCH 24p	CISCO SG102 -24	PSZ18111FHH
	ROUTER	MIKROTIK RB3011	
	FIREWALL	SOPHOS	S21005916BB217C
CATASTROS	SWITCH 24p	HP	CN6AGMZ0DNJ9983-60001
	SWITCH 24p	HP	CN247SW0Z4J9019-60101
BIBLIOTECA	SWITCH 24p	3COM	YECFC0RA033C0
	SWITCH 24p	DLINK	
SALA SESIONES	SWITCH 24p	HP	CNGAGMZ0W5J9983-60001
	SWITCH 24p	3COM	YECFBEP429500
PLANIFICACION	SWITCH 24p	CISCO	PSZ18111FHK
REGISTRO PROPIEDAD	SWITCH 24p	CISCO	
	ROUTER	MIKROTIK RB951UI-2HND	SN
AGUA POTABLE	SWITCH 24p	TPLINK	2155129001685
MERCADO ARGENTINA	SWITCH 16p	DLINK	
COMPLEJO LA MOYA	ROUTER	MIKROTIK RB951UI-2HND	SN
CAMAL MUNICIPAL	ROUTER	MIKROTIK RB951UI-2HND	SN

Elaborado Por:	JCVG	**Fecha:**	03-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	30-11-2018

N°	PRODUCTO	VERSIÓN	EDICIÓN	LICENCIA	INST/EN USO
1	Windows	7	Home Premium	Si	1
		Vista	Home Basic	Si	2
		Vista	Business	Si	2
		XP	Professional	Si	1
		XP	Home	Si	1
		10	Professional	Si	7
		7	Professional	Si	1
		8.1	Standard	Si	46
2	Office	2013	Standard	Si	43
		2007	Small Business	Si	1
		2010	Standard	Si	43
3	Windows Server	2003 R2	Standard	Si	1
		2008 R2	Standard	Si	2
				TOTAL	151

	PROGRAMA	VERSIÓN	LICENCIA
4	Adobe Acrobat 5.0	5.0	**No**
5	Adobe Flash Player 31 ActiveX	31.0.0.153	**No**
6	ESET NOD32 Antivirus	10.0.369.2	**No**
7	ERPCabildo32	2.00.0000	**-**
8	Google Chrome	71.0.3578.98	**No**
9	Mozilla FireFox ™	63.0.3 (x86 es-ES)	**No**
10	Internet Explorer ™	9.11.9600.18837	**No**
11	Windows Live Messenger	14.0.8050.1202	**No**
12	Windows Live Upload Toor	14.0.8014.1202	**No**

Elaborado Por:	JCVG	**Fecha:**	04-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	30-11-2018

4.2.2.4. Comunicación de Resultados

Objetivo General:

Presentar el Informe, una vez concluido el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

Objetivos Específicos:

1. Redactar el Informe de Auditoría a través de las conclusiones y recomendaciones emitidas en la fase de ejecución.
2. Emitir el Informe Final que exprese la opinión del auditor.

N°	Procedimiento	Referencia P/T	Elaborado por	Fecha
1	Elabore el Programa de Auditoria	**P/A 1/1**	JCVG	05-09-2018
2	Realice la Notificación de Finalización de Actividades	**N/FA 1/1**	JCVG	06-09-2018
3	Elabore la Convocatoria para Lectura del Informe	**C/LI 1/1**	JCVG	07-09-2018
4	Elabore la Carta de Presentación del Informe	**C/PI 1/2**	JCVG	12-09-2018
5	Elabore Informe de Auditoría Informática	**I/AI 1/12**	JCVG	12-09-2018

Elaborado Por:	JCVG	**Fecha:**	05-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

OFICIO N° 002- - FJVG-2018

Riobamba, 06 de septiembre de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

De nuestra consideración:

El motivo del presente es para comunicar que el equipo auditor ha finalizado las actividades con respecto al proceso de la Auditoría Informática, el mismo que se realizó conforme a las Normas Técnicas de Control Interno emitidas por la Contraloría General del Estado con respecto a la Norma 410 sobre Tecnologías de la Información y Comunicación.

Por lo que agradecemos su gentil colaboración y augurándole éxitos en sus funciones.

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	06-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

CONVOCATORIA

Pelileo, 07 de septiembre de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Ingeniero

Luis Carrasco

JEFE DE GESTIÓN TECNOLÓGICA DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

De nuestra consideración:

De acuerdo con lo dispuesto en el Programa de Auditoría y una vez concluido el proceso de Auditoría Informática, nos permitimos convocar a la reunión de lectura del Informe de Auditoría, que se llevará a cabo el día miércoles 12de septiembre del 2018 a las 15h00 en las instalaciones de la Ilustre Municipalidad, ubicado en la calle 22 de Julio y Padre Chacón.

Atentamente,

Ing. Willian Yanza

SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	07-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Pelileo, 12 de septiembre de 2018

Doctor

Manuel Caizabanda

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PELILEO

Presente

De nuestra consideración:

FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS, en uso de sus atribuciones legales, efectuó la Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, por el período comprendido entre el 1 de enero al 31 de diciembre de 2016.

Nuestra acción de control se llevó a cabo de acuerdo con las Normas Técnicas de Control Interno establecidas por la Contraloría General del Estado, específicamente la Norma 410 referente a Tecnología de Información y Comunicación. Estas normas requieren que el examen sea planificado y ejecutado para obtener certeza razonable de que la información y la documentación examinada no contienen exposiciones erróneas de carácter significativo, igualmente que las operaciones a las cuales corresponden, se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Responsabilidad de la Administración de TI

La administración es responsable por el manejo y buen funcionamiento de la Tecnología de la Información.

Responsabilidad del Auditor

Nuestra responsabilidad consiste en expresar una opinión sobre la Tecnología de la Información al ejecutar el examen de auditoría, el mismo que fue realizado bajo las Normas de Auditoría Generalmente Aceptadas y las Normas Técnicas de Control Interno.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en las conclusiones y recomendaciones que constan en el presente informe, las mismas que deben ser consideradas por las autoridades de la institución, con la finalidad de tomar las decisiones pertinentes.

Atentamente,

Ing. Willian Yanza
SUPERVISOR DE FÉNIX JVG AUDITORES & CONSULTORES ASOCIADOS

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

INFORME DE AUDITORÍA INFORMÁTICA

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

Entidad: GAD Municipal del Cantón San Pedro de Pelileo

Naturaleza del Trabajo: Auditoría Informática

Período: Del 1 de Enero al 31 de Diciembre de 2018

CAPÍTULO I

1.1.Motivo del Examen

Se efectuó la Auditoría Informática a la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo con el fin de evaluar la seguridad de la información.

1.2. Objetivos de la Auditoría

Objetivo General

Realizar una Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016, para evaluar la seguridad de la información.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Objetivos Específicos

- Analizar los riesgos que inciden en la seguridad de la información de la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.
- Identificar los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.
- Presentar el informe al concluir el proceso de la Auditoría Informática, que contemple las conclusiones y recomendaciones, que mejoren la seguridad de la información del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo.

1.3. Alcance de la Auditoría

El período que comprenderá la Auditoría Informática considera 1 de Enero al 31 de Diciembre del 2016.

1.4. Base Legal

La base legal que rige a la institución se puede apreciar a continuación:

- Constitución de la República del Ecuador
- Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD)
- Código de Trabajo
- Código de la Niñez y Adolescencia
- Ley Orgánica de la Función de Transparencia y Control Social
- Ley Orgánica del Servicio Público (LOSEP) y su Reglamento General (RGLOSEP)
- Ley Orgánica del Consejo de Participación Ciudadana y Control Social (CPCCS)

- Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su Reglamento General (RGLOSNCP)
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y su Reglamento
- Ley Orgánica de la Contraloría General del Estado y su Reglamento
- Normas Técnicas de Control Interno
- Estatuto Orgánico por Procesos institucional
- Reglamento de Talento Humano
- Reglamento de Seguridad y riesgos laborales

CAPÍTULO II

2.1.Resultados de la Auditoría Informática

Los resultados obtenidos de la Auditoría Informática realizada en el GAD Municipal del Cantón San Pedro de Pelileo se presentan a continuación:

La Unidad de Gestión Tecnológica depende de la Dirección Administrativa

Conclusión

La Unidad de Gestión Tecnológica al ser dependiente de la Dirección Administrativa provoca que los procesos tarden hasta esperar su aprobación de acuerdo a los trámites que realizan las diferentes unidades pertenecientes a la misma dirección, por lo que no se cumple con la Norma Técnica de Control Interno de la CGE, 410-01 Organización Informática.

Recomendación

Se recomienda al Alcalde y Concejo Municipal posicionar a Gestión Tecnológica en un nivel directivo independiente a fin que le permita efectuar las actividades de asesoría, apoyo y ayudar en la toma de decisiones organizacionales.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Plan Estratégico Informático desactualizado

Conclusión

El Plan Estratégico Informático no brinda información actualizada por lo que se convierte en un instrumento no válido a la hora de tomar decisiones, además no se cumple con la Norma Técnica de Control Interno de la CGE, 410 – 03 Plan informático estratégico de tecnología.

Recomendación

Se recomienda al Jefe de Gestión Tecnológica actualizar periódicamente el Plan Estratégico Informático de la Institución con el fin de proporcionar información veraz acerca del Gobierno Electrónico de GAD Municipal del Cantón San Pedro de Pelileo.

Falta de control de acceso a la Unidad de Gestión Tecnológica

Conclusión

La Unidad de Gestión Tecnológica no posee un control de acceso para el personal no autorizado lo que provocaría la pérdida de herramientas y el robo de la información, incumpliendo con lo que estipula la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.

Recomendación

Se recomienda el Jefe de la Unidad de Gestión Tecnológica controlar el acceso de personal no autorizado, mediante registros e identificaciones.

Señalética Insuficiente

Conclusión

La señalética de la Unidad al ser insuficiente provoca desinformación entre los usuarios tanto internos como externos, debido a la falta de presupuesto por lo que se debe solicitar en el POA para los siguientes años y cumplir con la Norma Técnica de Control Interno de la CGE, 410-09 Mantenimiento y control de la infraestructura tecnológica.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Recomendación

Se recomienda al Jefe de la Unidad de Gestión Tecnológica implementar en el POA la señalética que se requiere para la unidad.

Daños en el techo de la Unidad de Gestión Tecnológica

Conclusión

Las filtraciones de agua existentes en el edificio nuevo en donde se encuentra ubicada la Unidad de Gestión Tecnológica pueden llegar a dañar los equipos informáticos institucionales, debido a que no se consideró la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.

Recomendación

Se recomienda al Sr. Alcalde y al Jefe de la Unidad de Gestión Tecnológica tomar las respectivas medidas para evitar que las filtraciones de agua lleguen a dañar los equipos informáticos institucionales.

Inexistencia de cámaras de seguridad en la Unidad de Gestión Tecnológica

Conclusión

La Unidad de Gestión Tecnológica cuenta con cámaras de seguridad por lo que incide en la pérdida de equipos informáticos y herramientas e incumpliendo con la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.

Recomendación

Se recomienda al Jefe de la Unidad de Gestión Tecnológica formular un proyecto para la implementación de cámaras de vigilancia para garantizar la seguridad física interna e implementar en el POA para los próximos años.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Ubicación del Centro de Procesamiento de Datos

Conclusión

El área en donde se encuentra el Centro de Procesamiento de Datos está adecuada de acuerdo al presupuesto asignado por lo que reduce el espacio y el personal que labora en dicha área debe adaptarse al ruido que genera y no se cumple con la Norma Técnica de Control Interno de la CGE, 410-08 Adquisición de infraestructura tecnológica.

Recomendación

Se recomienda al Sr. Alcalde y al Jefe de la Unidad de Gestión Tecnológica tomar las respectivas medidas para propiciar una infraestructura adecuada para el Centro de Procesamiento de Datos a fin de salvaguardar la integridad, confiabilidad y disponibilidad de la información institucional.

Pólizas de seguros para el Centro de Procesamiento de Datos y equipos informáticos

Conclusión

El Centro de Procesamiento de Datos y los equipos informáticos que no cuentan con una póliza de seguros en caso de suscitarse un desastre o casos fortuitos se perderían los equipos parcial o totalmente y poniendo en riesgo la integridad, confiabilidad y disponibilidad de la información. Además la póliza de seguros es una medida de seguridad física para los equipos informáticos. Finalmente no se cumple con la Norma Técnica de Control Interno de la CGE, 410-10 Seguridad de tecnología de información.

Recomendación

Se recomienda al Jefe de Gestión Tecnológica implementar en los requerimientos del POA la póliza de seguros, de igual forma al Jefe de Compras públicas implementar en el PAC la póliza de seguros para equipos informáticos.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Inexistencia de una política para dar de baja los equipos informáticos

Conclusión

La falta de una política para dar de baja los equipos informáticos produce una inadecuada gestión de los mismos después de haber terminado su vida útil y no se lleva a cabo lo que especifica la Norma Técnica de Control Interno de la CGE, 410-04 Políticas y procedimientos.

Recomendación

Se recomienda al personal de la Unidad de Gestión Tecnológica y al personal de bodega formular y establecer una política para dar de baja los equipos informáticos al haber cumplido su vida útil con el propósito de darle un mejor fin que contribuya al cuidado del medio ambiente y no provocar la acumulación de los mismos.

Los respaldos de la información no son guardados en algún sitio o ciudad del país

Conclusión

La Unidad de Gestión Tecnológica salvaguarda la información mediante el uso de la nube y discos duros, sin embargo para garantizar la disponibilidad e integridad de la misma es necesario contratar los servicios de empresas que guardan la información en sitios externos o ciudades del país.

Recomendación

Se recomienda al Jefe de Gestión Tecnológica implementar en los requerimientos del POA la contratación de servicios de empresas a fin de salvaguardar la información en lugares externos o ciudades del país para garantizar la disponibilidad e integridad de la información institucional.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

Inutilización de claves fuertes por parte de los funcionarios

Conclusión

Los funcionarios no utilizan contraseñas fuertes para encender el computador, tampoco para ingresar al sistema Cabildo ERP para el desarrollo de sus actividades laborales, exponiéndose al robo de información e incumpliendo con la Norma Técnica de Control Interno de la CGE, 410-12 Administración de soporte de tecnología de información.

Recomendación

Se recomienda a los funcionarios del GAD Municipal del Cantón San Pedro de Pelileo utilizar contraseñas fuertes que incluyan al menos 14 caracteres alfanuméricos y caracteres especiales como medida de seguridad para evitar el robo de información confidencial.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

2.2.Resultados de los Indicadores

A continuación se presentan los resultados de los indicadores aplicados en la Auditoría Informática al GAD Municipal del Cantón San Pedro de Pelileo:

INDICADORES DE EFICIENCIA				
NOMBRE DEL INDICADOR	**FÓRMULA**	**CÁLCULO**	**RESULTADO**	**ANÁLISIS**
Porcentaje de computadoras obsoletas	(Número de computadoras obsoletas en la Institución en el período 2016/Total de computadoras en la Institución en el período 2016)*100	(34/134)*100	25	El número de computadoras obsoletas representa al 25% las mismas que fueron dadas de baja y almacenadas en la bodega municipal. Con el mantenimiento correctivo respectivo se cambian las piezas defectuosas, sin embargo si no se encuentra solución se reemplaza el equipo.
Porcentaje de portátiles obsoletas	(Número de portátiles obsoletas en la Institución en el período 2016/Total de portátiles en la Institución en el período 2016)*100	(2/17)*100	11.77%	El número de computadoras portátiles obsoletas representa al 111.77% las mismas que fueron dadas de baja y almacenadas en la bodega municipal.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

NOMBRE DEL INDICADOR	FÓRMULA	CÁLCULO	RESULTADO	ANÁLISIS
Porcentaje de Impresoras obsoletas	(Número de impresoras obsoletas en la Institución en el período 2016/Total de impresoras en la Institución en el período 2016)*100	(41/107)*100	38%	El número de impresoras obsoletas representa al 38% las mismas que fueron dadas de baja y almacenadas en la bodega municipal. Para el mantenimiento de las impresoras se requiere contratar un servicio externo debido a la naturaleza del trabajo y reemplazo de partes.
INDICADORES DE EFICACIA				
Soporte Técnico	(Número de asistencias técnicas atendidas en el período 2016/Número de asistencias técnicas solicitadas en el período 2016) *100	(1200/1220)*100	98.361	Con respecto al soporte técnico, los técnicos del área de Gestión Tecnológica reciben en promedio 5 llamadas telefónicas a diario, lo que representa 1200 asistencias en el año las mismas que son atendidas en el 98%

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

NOMBRE DEL INDICADOR	FÓRMULA	CÁLCULO	RESULTADO	ANÁLISIS
Ejecución de proyectos	(Número de proyectos ejecutados en el período 2016/Número de proyectos planificados en el período 2016)*100	(6/8)*100	75	De acuerdo al POA 2016 presentado por la Unidad de Gestión Tecnológica se plantearon 8 proyectos de los cuales se cumplieron 6 durante el año, debido a la falta de presupuesto, lo que representa el 75% en ejecución de proyectos
Acceso a Internet	(Número de computadoras que tienen acceso a internet en el período 2016/Total de computadoras en el período 2016)*100	(149/159)*100	93.71	Con respecto al acceso a internet, el 93,71% de computadoras tienen acceso a internet, esto se debe a que 10 computadoras que se encuentran en la biblioteca tienen acceso a internet ocasionalmente.
INDICADORES PRESUPUESTARIOS				
% de Participación del Presupuesto de la Unidad de Gestión Tecnológica	(Total del presupuesto asignado para la Unidad de Gestión Tecnológica en el período 2016/Total del presupuesto del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	($56.749,35/ $27'391.396,26)*100	0.21	El porcentaje de participación del presupuesto de la Unidad de Gestión Tecnológica con respecto al total del presupuesto institucional corresponde al 0,21% esto se debe a que dicha Unidad depende de la Dirección Administrativa.

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

NOMBRE DEL INDICADOR	FÓRMULA	CÁLCULO	RESULTADO	ANÁLISIS
% de Participación del Presupuesto de la Dirección Administrativa	(Total del presupuesto asignado para la Unidad de Gestión Tecnológica en el período 2016/Total del presupuesto asignado para la Dirección Administrativa en el período 2016)*100	($56.749,35/ $327.711,81) *100	17.32	El porcentaje de participación del presupuesto de la Unidad de Gestión Tecnológica con respecto al presupuesto de la Dirección Administrativa corresponde al 17,32% esto se debe a que dicho programa comprende Unidades como Contratación Pública, Talento Humano, Servicios Generales y Salud Ocupacional.
INDICADORES DE SEGURIDAD				
Seguridad Lógica	(Número de computadoras que cuentan con la contraseña fuerte para ser encendidas en el período 2016/Total de computadoras del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	(62/162)*100 %	38%	Con respecto a la seguridad lógica apenas el 38% de servidores/as usan una contraseña fuerte para encender el computador.
	(Número de computadoras que cuentan con screensaver o protector de pantalla en el período 2016/Total de computadoras del GAD Municipal del Cantón San Pedro de Pelileo en el período 2016)*100	(65/162)*100 %	38%	Con respecto a la seguridad lógica apenas el 38% de servidores/as usan en sus computadoras el protector de pantalla o screensaver

Elaborado Por:	JCVG	**Fecha:**	12-09-2018
Revisado Por:	WGYCH/CVBP	**Fecha:**	05-12-2018

CONCLUSIONES

El presente trabajo de investigación contemplan las siguientes conclusiones:

- La Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo se encuentra expuesta a riesgos que afectan a la seguridad física y lógica que han sido tratadas en el presente trabajo de investigación que inciden en la integridad, confiabilidad y disponibilidad de la información.

- Los procesos que realiza la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo con respecto a los equipos informáticos se basa en la estandarización, es por esta razón que al realizar los mantenimientos correctivos se reemplazan con equipos de características similares con la finalidad de no afectar la continuidad de las labores de los funcionarios.

- El centro de procesamiento de datos no se encuentra bajo estándares, además las instalaciones físicas carecen de seguridades como cámaras de seguridad o registros para el acceso al lugar, exponiendo a la Unidad de Gestión Tecnológica a robos o sabotajes.

- El Informe Final de Auditoría dirigido hacia la máxima autoridad y jefe de la unidad auditada conlleva a la toma de decisiones con el fin de mejorar las condiciones de las instalaciones físicas y asegurar que la información institucional no se vea amenazada por hackers o crackers.

RECOMENDACIONES

A continuación se puede apreciar las recomendaciones del presente trabajo de investigación:

- Se recomienda al personal de la Unidad de Gestión Tecnológica realizar las gestiones necesarias a fin de salvaguardar la información, así como su disponibilidad, confiabilidad e integridad, también garantizar el buen uso y protección de los equipos informáticos, además los funcionarios de la institución deben acatar las políticas institucionales como cambio de claves periódicos que posean mínimo 8 caracteres incluyendo el uso de signos de puntuación.

- Se recomienda al personal de la Unidad de Gestión Tecnológica elaborar los proyectos para implementar las cámaras de seguridad y vigilancia en el área, también efectuar el registro de ingreso para proteger los bienes e información de la Unidad.

- Se recomienda aplicar estándares como las ISO 27001 o ANSI TIA 942 en la que es especifica los niveles de TIER, con respecto al Centro de Procesamiento de Datos con el fin de salvaguardar la integridad de la información y garantizar un espacio físico adecuado.

- Se recomienda al Señor Alcalde, Concejo Municipal y Dirección Administrativa dar mayor participación a la Unidad de Gestión Tecnológica, en la estructura organizacional ubicándola como un departamento, a fin que reciba los recursos suficientes para llevar a cabo los proyectos que beneficien a la institución y contribuyan con su desarrollo.

BIBLIOGRAFÍA

Advisera Expert Solutions Ltd. (s/f). *ISO 27001*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Alatrista, M. Á. (17 de Noviembre de 2015). *Técnicas de Auditoría*.[Entrada de blog]. Obtenido de https://www.auditool.org/blog/auditoria-externa/2158-tecnicas-y-procedimientos-de-auditoria-lo-que-todo-auditor-debe-conocer

Asociación Española para la calidad. (2018). *COSO*. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/coso

Chicano, E. (2014). *Auditoría de Seguridad Informática.* España: IC Editorial.

Contraloría General del Estado. (2014). *Normas Técnicas de Control Interno.* Obtenido de http://www.oas.org/juridico/pdfs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Costas, J. (2014). *Seguridad Informática.* Madrid: RA-MA.

Escrivá, G., Romero, R., Ramada, D. J., & Onrubia, R. (2013). *Seguridad Informática.* España: Macmillan Iberia, S.A.

Espino, G. (2014). *Fundamentos de Auditoría.* México: Grupo Editorial Patria .

Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo. (2018). *Directorio de la Institución.* Obtenido de http://pelileo.gob.ec/html/images/lotaip2018/febrero/Literal_b1-Directorio_de_la_institucion.pdf

Grupo Confitel Andino. (2014). *Data Center: El Estándar TIA 942*. Obtenido de https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

Hidalgo Jácome, M. R., & Ortega Acosta, M. F. (mayo de 2014). *Aplicación de una Auditoría Informática a la seguridad física a los equipos de computo del GAD Municipal del Cantón Salcedo ubicado en la Provincia de Cotopaxi durante el periodo 2011*.(Tesis de pregrado, Universidad Técnica de Cotopaxi). Obtenido de http://repositorio.utc.edu.ec/handle/27000/1961

Huatangare , D. (2015). *Interpretación de las Normas de Auditoría Generalmente Aceptadas*. [Entrada de blog]. Obtenido de http://informe-nagas.blogspot.com/2015/09/normas-de-auditoria-generalmente.html

IT Governance Institute. (2007). *COBIT 4.1*. Obtenido de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf

Lara, Y. (31 de enero de 2017). *Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Guano, Provincia de Chimborazo, período 2015*. (Tesis de pregrado, Escuela Superior Politécnica de Chimborazo). Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6293

Marulanda, L. (2016). *Hallazgo de Auditoría.* Obtenido de https://www.contraloriabga.gov.co/files/HALLAZGOS_LEMT.pdf

Matías, M. (2017). *Marco referencial ITIL: ventajas y desventajas*. [Entrada de blog]. Obtenido de http://itilmmatiasc.blogspot.com/2017/05/ventajas-y-desventajas-de-itil.html

Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México: Pearson Educación.

Pallerola , J., & Monfort, E. (2014). *Auditoría.* Madrid: RA-MA.

Piattini, M., & Del Peso, E. (2001). *Auditoría Informática: Un enfoque práctico* (2da ed.). Madrid: Alfaomega RA-MA.

Roa, J. F. (2013). *Seguridad Informática.* Madrid: McGraw-Hill/ Interamericana de España, S.L.

Segu.Info Seguridad de la Información. (2009). *Niveles de Seguridad Lógica.* Obtenido de https://www.segu-info.com.ar/logica/seguridadlogica.htm

Servicio Nacional de Contratación Pública. (2016). *PAC 2016 GAD Municipal del Cantón San Pedro de Pelileo*. Obtenido de https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/buscarPACe.cpe?entidadPac=Si1mDZvTcoFxX318fjj9VqLsSMFeFHq1e3_5vCctr-g,&anio=ZPCKDty9dARNyYfX2G4yVLYnhYZETq-x1cgvyrudCuw,&nombre=CQ7ztMPFTbYqeEOnB-MqifNIYffsXCE39dzXatk0QN92yM1JT4ShFVdwOqjUX

Tamayo , J. A., & Tamayo, A. (s/f). *La Seguridad Física en los Centros de Informática.* Obtenido de http://bdigital.unal.edu.co/57849/1/laseguridadfisicaenloscentrosdeinformatica.pdf

Tapia, C., Guevara, E., Castillo, S., Rojas, M., & Salomón , L. (2016). *Fundamentos de Auditoría. Aplicación práctica de las Normas Internacionales de Auditoría.* México: IMCP (Instituto Mexicano de Contadores Públicos).

Velázquez, A. I. (18 de Agosto de 2011). *Análisis del Riesgo*. [Entrada de blog]. Obtenido de http://aplicaciondeseguridadinformatica.blogspot.com/2011/08/b-clasificacion-de-los-principales.html

Velin Jara, J. G. (05 de junio de 2016). *Auditoría Informática al Gobierno Autónomo Descentralizado Municipal de Pastaza, período 2014.* (Tesis de pregrado, Escuela Superior Politécnica de Chimborazo). Obtenido de http://dspace.espoch.edu.ec/handle/123456789/5937

ANEXOS

Anexo N° 1: Encuesta Aplicada al Personal de la UGT

ENCUESTA

Dirigida al personal de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo

1. **El acceso al lugar donde se ubica el área de sistemas está restringido para el personal no autorizado.**

   Si ☐ No ☐

2. **El área de sistemas cuenta con cámaras de seguridad internas y externas?**

   Si ☐ No ☐

3. **El Centro de Procesamiento de Datos dispone de aire de precisión para regular la temperatura?**

   Si ☐ No ☐

4. **El lugar donde se ubica el área de sistemas cuenta con una salida de emergencia?**

   Si ☐ No ☐

5. **El lugar donde se ubica el área de sistemas cuenta con sensores de humo?**

   Si ☐ No ☐

6. **La señalética del área de sistemas es suficiente y se encuentra visible?**

   Si ☐ No ☐

7. **Los puntos del centro de datos están debidamente aterrizados (conexión a tierra)?**

   Si ☐ No ☐

8. **Usted participa de los programas de capacitación institucionales?**

   Si ☐ No ☐

9. **Las computadoras de la institución cuentan con una póliza de seguros?**

   Si ☐ No ☐

10. **La planificación para el área de sistemas se encuentra debidamente documentado?**

    Si ☐ No ☐

Anexo N° 2: Encuesta Aplicada a los funcionarios/as del GAD Municipal del Cantón San Pedro de Pelileo

ENCUESTA

Objetivo: Recabar información para la realización de la Auditoría Informática al GAD Municipal del Cantón San Pedro de Pelileo.

1. **Usted como califica la atención que brinda el personal del área de sistemas:**

Excelente ☐ Muy Buena ☐ Buena ☐ Regular ☐ Mala ☐

2. **El sistema que utiliza para el desarrollo de sus actividades laborales es:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

3. **Considera que las políticas sobre el uso de los equipos informáticos en su lugar de trabajo son:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

4. **Cómo califica el servicio de internet que brinda el GAD Municipal del Cantón San Pedro de Pelileo?**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

5. **Considera que la utilización de claves fuertes para encender el computador es una medida de seguridad:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

6. **Como califica la utilización de claves fuertes para ingresar al sistema informático Cabildo?**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

7. **Cada qué tiempo realiza la renovación de claves personales para uso del sistema?**

Cada mes ☐ Cada tres meses ☐ Cada seis meses ☐ Cada año ☐ Nunca ☐

8. **Considera que la utilización de políticas institucionales para la renovación de claves personales es:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

9. **Considera que el plan de contingencias y medidas de seguridad ante riesgos que ocasionen daño a los equipos informáticos son:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

10. **Cómo califica su lugar de trabajo si cuenta con los equipos necesarios como UPS con regulador de voltaje que permita continuar en sus actividades en caso de corte de energía:**

Excelente ☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐

Anexo N° 3: Entrevista al Jefe de la Unidad de Gestión Tecnológica

ENTREVISTA AL JEFE DE LA UNIDAD DE GESTIÓN TECNOLÓGICA DEL GAD MUNICIPAL DEL CANTÓN SAN PEDRO DE PELILEO

Entrevistado: Ing. Luis Carrasco

1. **Cuántas personas trabajan en el área de sistemas y qué cargos desempeñan?**
2. **Se ha establecido algún tipo de planificación para el área de sistemas?**
3. **Cuentan con planes de mantenimiento preventivo y correctivo de equipos informáticos, de redes y comunicaciones del Gobierno de San Pedro de Pelileo?**
4. **Cada qué tiempo se realiza el mantenimiento de los recursos informáticos?**
5. **Existe alguna política para el uso de los recursos informáticos?**
6. **Existe un inventario de los recursos informáticos y quien es el responsable de mantenerlo actualizado?**
7. **Se realizan copias de los archivos en algún lugar distinto a los computadores?**
8. **Se ejecutaron los proyectos planteados en el POA 2016?**

A continuación se muestra las fotos de la Unidad de Gestión Tecnológica del GAD Municipal del Cantón San Pedro de Pelileo:

Anexo N° 4: Ingreso a la Unidad de Gestión Tecnológica

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

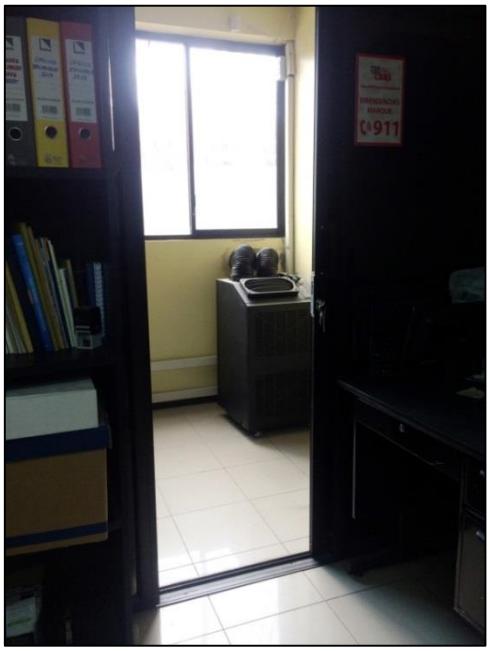
El ingreso a la Unidad de Gestión Tecnológica se encuentra junto a las ventanillas de recaudación.

Anexo N° 5: Parte externa de la Unidad de Gestión Tecnológica

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

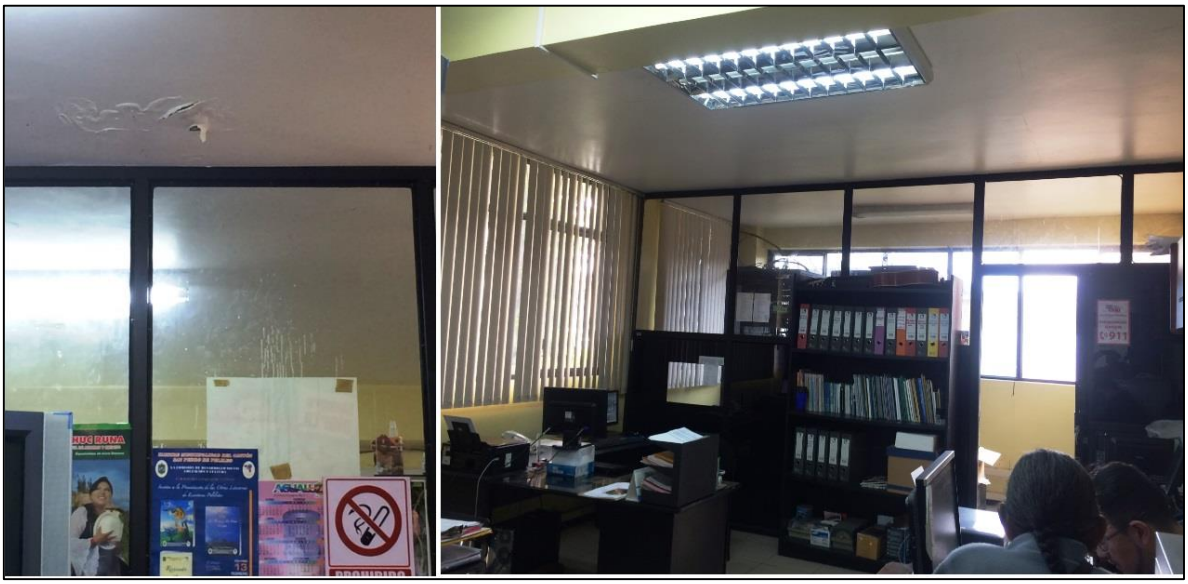
En la imagen se puede apreciar la parte externa de la Unidad de Gestión Tecnológica que se encuentra junto a la ventanilla de Tesorería.

Anexo N° 6: Área de la Unidad de Gestión Tecnológica



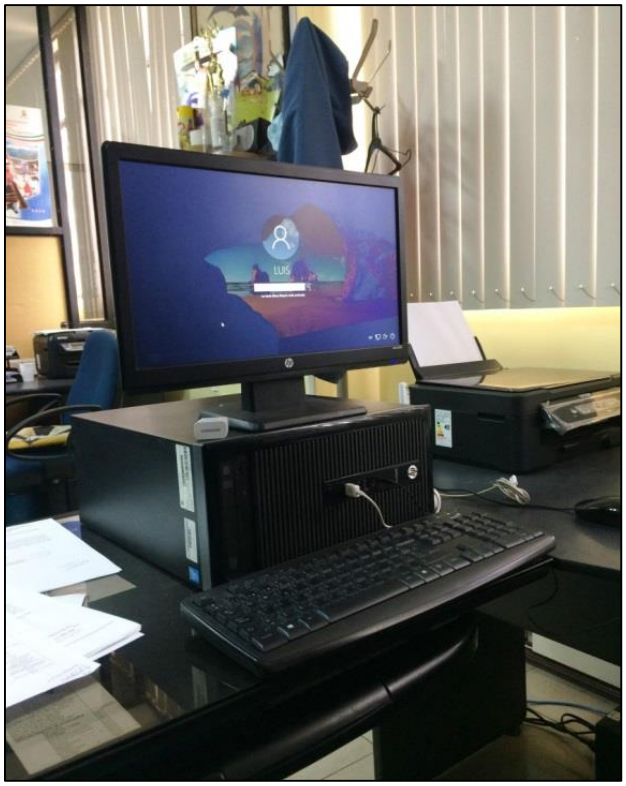
Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 7: Techo e iluminación de la UGT



Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 8: Uso del Protector de pantalla en la UGT



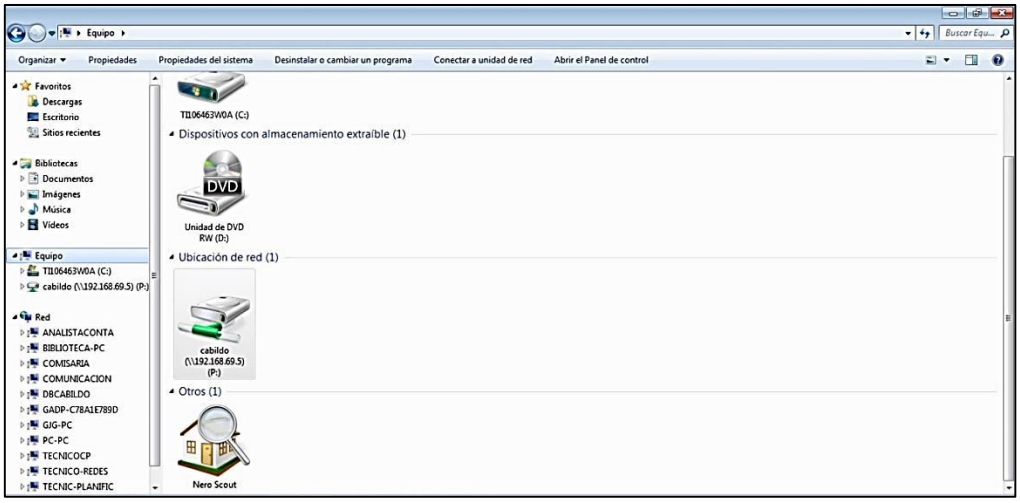
Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 9: Ingreso al Sistema ERP Cabildo

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

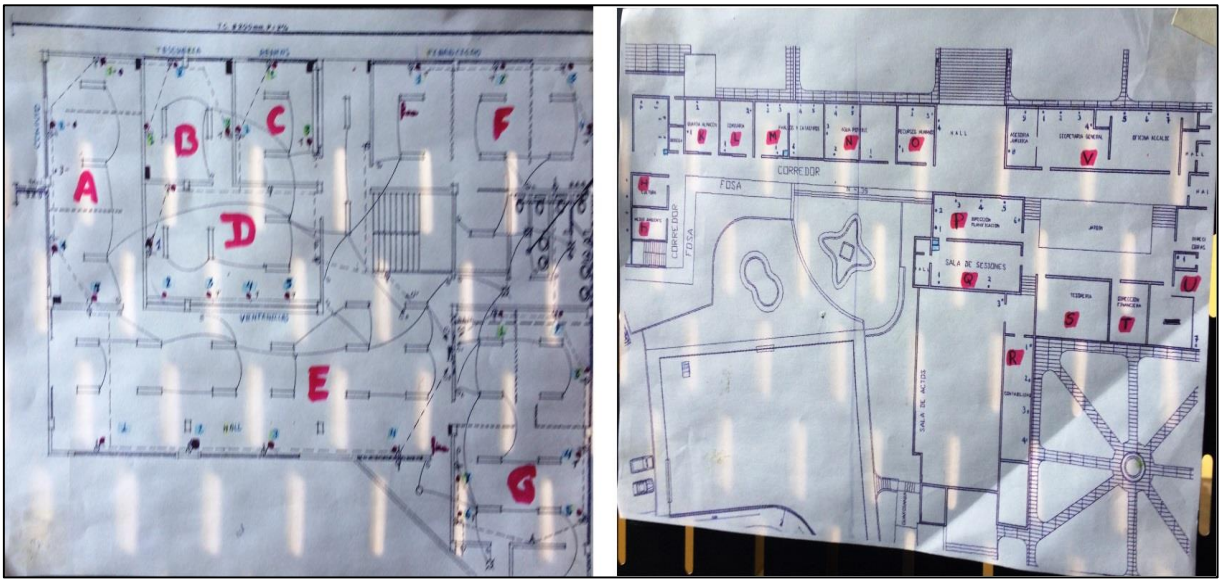
Como se puede observar en la imagen que corresponde a la pantalla inicial del Sistema Integrado de Gestión ERP Cabildo, mediante el cual los funcionarios del GADMC Pelileo llevan a cabo sus respectivas funciones.

Anexo N° 10: Red LAN



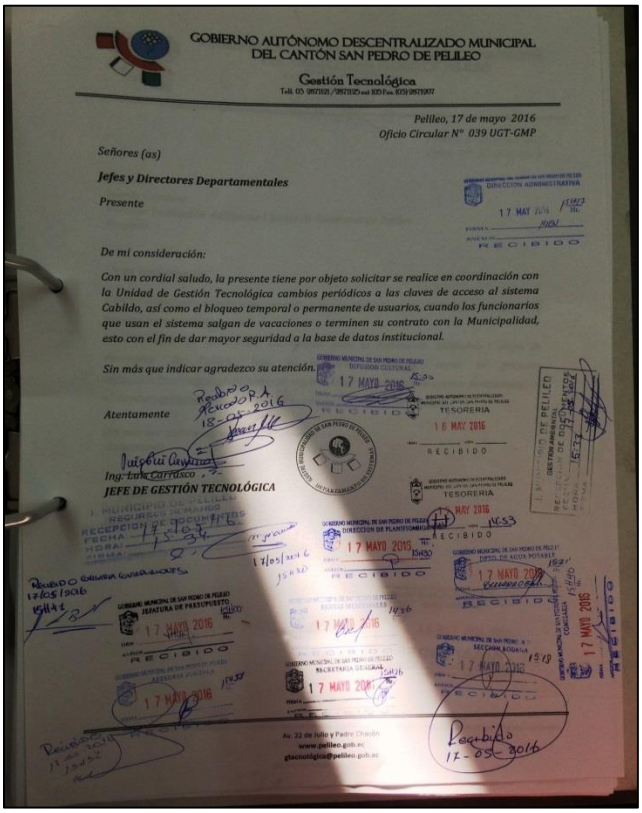
Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 11: Puntos de red del GADMSPP



Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 12: Oficio en el cual denota el cambio de contraseñas



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL
DEL CANTÓN SAN PEDRO DE PELILEO

Gestión Tecnológica

Pelileo, 17 de mayo 2016
Oficio Circular N° 039 UGT-GMP

Señores (as)

Jefes y Directores Departamentales

Presente

De mi consideración:

Con un cordial saludo, la presente tiene por objeto solicitar se realice en coordinación con la Unidad de Gestión Tecnológica cambios periódicos a las claves de acceso al sistema Cabildo, así como el bloqueo temporal o permanente de usuarios, cuando los funcionarios que usan el sistema salgan de vacaciones o terminen su contrato con la Municipalidad, esto con el fin de dar mayor seguridad a la base de datos institucional.

Sin más que indicar agradezco su atención.

Atentamente

Ing. Luis Carrasco
JEFE DE GESTIÓN TECNOLÓGICA

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 13: Equipos obsoletos ubicados en la bodega municipal

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 14: Equipos de red del cableado estructurado

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

Anexo N° 15: POA 2016 Unidad de Gestión Tecnológica

GOBIERNO MUNICIPAL DE PELILEO
PLAN OPERATIVO ANUAL
EJERCICIO ECONOMICO 2016

DIRECCION: ADMINISTRATIVA

UNIDAD: GESTION TECNOLOGICA

OBJETIVO: Planear, coordinar y supervisar el crecimiento y administración de los Sistemas Integrales y de las Redes de Datos, de Aplicaciones Municipales y sus servicios integrados

ESTRATEGIAS: Gestionar, implementar y difundir el uso de nuevas tecnologías en el trabajo diario e incentivar su aplicación a través de capacitaciones al personal administrativo.

META: Crear una Unidad Tecnológica centralizada y automatizada de información acorde a los métodos y aplicaciones de la Era Actual

PROYECTO	ACTIVIDADES	Cronograma CUATRIMESTRE 1	2	3	EQUIPO NECESARIO (Material y Humano)	COSTO USD	BENEFICIARIOS	FINANCIAMIENTO	RESPONSABLES	INIDICADORES DE GESTION	MEDIOS DE VERIFICACION
Mantenimiento de equipos de impresión	Verificar el inventario de software. Solicitar visto bueno para iniciar el proceso de adquisición. Adquirir las licencias a través del Portal de Compras Públicas Activar las licencias adquiridas en los equipos informáticos	x	x	x	Servicio técnico especializado	5000 ✓ 530204	Usuarios y Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Revisión, mantenimiento preventivo y cambio de partes sensibles de las impresoras	Equipos de impresión funcionando correctamente
Pago y mantenimiento de la Red WIFI en los parques urbanos	Revisión de los equipos de activos de red. Pruebas de conectividad y respuesta de trsmisión de datos. Solicitar equipos activos de red de remplazo en caso de haber averias. Instalación y configuración de nuevos equipos activos de red.	x	x	x	Equipos activos de red, Funcionarios de Tecnologia	10000 Ubicado en otro programa 341	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Equipos conectados a la red local	Eficiente conexión a la red municipal
Soporte al Sistema Integral de Gestión Municipal Cabildo	Solicitar autorización y presupuesto al Alcalde. Solicitar requerimientos de automatización a las Unidades Municipales Automatizar los requerimientos institucionales Respaldar la información y ejecutar el mantenimiento anual al sistema.	X	X	X	Funcionarios de Tecnologia y técnicos de PrisHard	6000 ?	Usuarios y Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica, Avaluos, Tesorería, Dir. Financiera, Agua Potable	Sistema funcionando adecuadamente Unificación de Codigos de Identificación Unico Transacciones realizadas sin inconvenientes Reducción de tiempo al realizar los trámites	Sostenibilidad al Software implementado

PROYECTO	ACTIVIDADES	Cronograma CUATRIMESTRE 1	2	3	EQUIPO NECESARIO (Material y Humano)	COSTO USD	BENEFICIARIOS	FINANCIAMIENTO	RESPONSABLES	INIDICADORES DE GESTION	MEDIOS DE VERIFICACION
Adquisición de repuestos y partes informáticas	Diagnostico de las partes mas vulnerables Solicitar la adquisición de acuerdo a los modelos existentes Reposición de los dispositivos dañados	X			Repuestos y Técnico Municipal	3000 ✓ 531407	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Gestión Tecnológica	Cambios realizados en equipos que superan en prmedio los dos años de funcionamiento	Equipos informáticos operativos
Capacitación en cursos y talleres tecnológicos (ORACLE, PLSQL, SEGURIDAD INFORMATICA)	Solicitar autorización para la participación en eventos de capacitación Asistir a cursos y talleres Aplicar los conocimientos en las tareas diarias del trabajo	X	X	X	Personal Municipal	3000 ?	Funcionarios de la municipalidad	Presupuesto Municipal	Jefatura de Gestión Tecnológica	Nuevas técnicas en los procesos informáticos	Personal capacitado en las nuevas tecnologias
Plan de mantenimiento de equipos informáticos	Presentar el Plan Anual de Mantenimiento de equipos informáticos Comunicar el cronograma de mantenimiento a las Unidades Municipales Adquirir herramientas Ejecutar el plan de mantenimiento	X	X	X	Herramientas, respuestos, Funcionarios Municipales	2000 530204 Sobrante	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Jefatura de Gestión Tecnológica	Bitacoras con información de los equipos. Informes semestrales	Equipos informaticos en buen funcionamiento
Consulta gráfica de predios en la web	Adquisición de servidor $3.000 Contratacion para el desarrollo de la aplicación de consulta Facilitar la información respectiva Acoplar la aplicación al sitio web municipal		X		Portal Web, Servidor, Aplicación de consulta	? 10000 Próximo	Avaluos y catastros, Ciudadanía en general	Presupuesto Municipal	Unidades de Tecnologia y Avaluos y Catastros	Aumentar el espacio de alojamiento y renovar el dominio gubernamental	Portal web de consulta en linea
Licencia de firewall	Determinar el tráfico de datos en la red Adquirir el modelo de firewall mas idòneo Contratar el alojamiento y diseño del sitio Configuraciòn del equipo			X	Equipo firewall Funcionarios de la Municipalidad	4000 ✓ 530102	Funcionarios que operan Computador en el GAD Municipal de Pelileo	Presupuesto Municipal	Unidad de Tecnologia	Equipo adquirido y configurado	Control efectivo de spam y correo no deseado en las pàginas web y correos electrònico respectivamente

A. RECURSOS DE PERSONAL

GRUPO OCUPACIONAL	Número de Servidores		ASIGNACIÓN ANUAL	Número de Servidores		ASIGNACIÓN ANUAL
	Disponible	RMU		Requerido	RMU	
Directivo			-			-
Profesional			-			-
Técnico	1	817,00	9.804,00			-
Administrativo			-			-
Servidor Público de Apoyo			-			-
Servidor Público de Servicios			-			-
			9.804,00			-
Total RMU LOSEP:						**9.804,00**
Jornales Ocasionales			-			-
Jornales Permanentes			-			-
			-			-
Total RMU Código de Trabajo:						-
TOTAL GENERAL US$...						**9.804,00**

B. RECURSOS EN SUMINISTROS Y MATERIALES

CÓDIGO	DETALLE	UNIDAD DE MEDIDA	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0804	**MATERIALES DE OFICINA**				
	Papel bond A4	resma	10	3,50	35,00
	Esferográfico punta gruesa color azul	u	20	0,80	16,00
	Frasco de tinta negro EPSON	u	5	10,00	50,00
	Frasco de tinta amarillo EPSON	u	2	10,00	20,00
	Frasco de tinta azul EPSON	u	2	10,00	20,00
	Frasco de tinta rojo EPSON	u	2	10,00	20,00
	Lapiceros	u	5	4,00	20,00
	Archivador tamaño oficio	u	10	3,50	35,00
	Resaltador varios colores fosforescentes	u	3	1,20	3,60
	Tijera pequeña	u	1	1,50	1,50
	Portapapeles de 3 pisos	u	3	10,00	30,00
	Memory flash 16 GB	u	3	20,00	60,00
	Torre de 100 CD IMATION	u	1	50,00	50,00
	Torre de 100 DVD IMATION	u	1	80,00	80,00
	Subtotal US$...				**441,10**
0805	**MATERIALES DE ASEO**				
	Franela	metro	3	2,00	6,00
	Guaipe	funda	3	5,00	15,00
	Jabón liquido	galón	1	15,00	15,00
	esboba y pala con mango	u	1	15,00	15,00
	Basurero metalico	u	1	20,00	20,00
	Subtotal US$...				**71,00**
0806	**HERRAMIENTAS**				
	Juego de llaves	u	1	80,00	80,00
	Juego de desarmadores planos	u	1	80,00	80,00
	Alicate	u	1	20,00	20,00
	Juego de desarmadores estrellas	u	1	80,00	80,00
	Juego de desarmadores hexagonales	u	1	80,00	80,00
	Taladro	u	1	200,00	80,00
	Subtotal US$...				**420,00**
0809	**MEDICAMENTOS**				
	Subtotal US$...				-
0811	**MATERIALES DE CONSTRUCCIÓN, ELÉCTRICOS, PLOMERÍA, CARPINTERÍA**				
	Subtotal US$...				-
0813	**REPUESTOS Y ACCESORIOS**				
	Fuente de poder 600 WATTS	u	10	30,00	300,00
	Disco duro SATA 500 GB	u	5	120,00	600,00
	Regulado de voltaje	u	5	20,00	100,00
	Teclado USB	u	10	15,00	150,00
	Rollo de Cable UTP 5e	u	1	100,00	100,00
	Conectores RJ45	u	100	0,30	30,00
	Mouse USB	u	10	10,00	100,00
	Subtotal US$...				**1.380,00**
0819	**ACCESORIOS E INSUMOS QUÍMICOS Y ORGÁNICOS**				-
	Subtotal US$...				-
	TOTAL US$...				**2.312,10**

F. GASTOS EN INFORMÁTICA

CÓDIGO	DETALLE	CANTIDAD	PRECIO	ASIGNACIÓN ANUAL
0701	**DESARROLLO, ACTUALIZACIÓN, ASISTENCIA TÉCNICA Y SOPORTE DE SISTEMAS INFORMÁTICOS**			
	Asistencia técnica sistema CABILDO	1	6.000,00	6.000,00
	Subtotal US$...			**6.000,00**
0702	**ARRENDAMIENTOS Y LICENCIAS DE USO DE PAQUETES INFORMÁTICOS**			
	Renovación licencia Firewall	1	4.000,00	4.000,00
	Pago de internet en zonas Wifi Urbanos	3	2.500,00	7.500,00
	Subtotal US$...			**11.500,00**
0704	**MANTENIMIENTO Y REPARACIÓN DE EQUIPOS Y SISTEMAS INFORMÁTICOS**			
	Mantenimiento impresoras del GAD	95	50,00	4.750,00
	Mantenimiento generador electrico	2	500,00	1.000,00
	Mantenimiento de zonas Wifi Urbanos	1	2.500,00	2.500,00
	Mantenimiento aire acondicionado	1	150,00	150,00
	Subtotal US$...			**8.400,00**
	TOTAL US$...			**25.900,00**

Nota: Indicar de donde se toma los precios referenciales

Fuente: GAD Municipal del Cantón San Pedro de Pelileo

A continuación se puede observar el PAC 2016 del GAD Pelileo consultado a través del portal de Compras Públicas (2016):

Anexo N° 16: PAC 2016

Sistema Oficial de Contratación Pública

Consulta del Plan Anual de Contratación

Entidad: GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON SAN PEDRO DE PELILEO
Año de Adjudicación: 2016
Valor Asignado: $ 30,603,242.0100

Nro	Partida Pres	CPC	T. Comp	T. Régi en	Fon d B	Tipo de Presupu o	Tipo de Produc	Cat. Electr ico	Procedimient o	Descripció n	Car	U. Med a	Costo	V. Tot		Períod
27	361770201	713340318	Servicio	Común	NO	Proyecto de Inversión	No Normalizado	NO	Licitación	Seguros	1.00	Unidad	35,000.00	35,000.00		C1 C2 C3
100	342570201	713340318	Servicio	Común	NO	Gasto Corriente	Normalizado	NO	Subastas Inversa Electrónica	Seguros	1.00	Unidad	13,000.00	13,000.00		C1 C2 C3
120	341570201	713340318	Bien	Común	NO	Gasto Corriente	Normalizado	NO	Infima Cuantía	Seguros	1.00	Unidad	1,200.00	1,200.00		C1 C2 C3
288	112570201	713310011	Servicio	Común	NO	Proyecto de Inversión	No Normalizado	NO	Menor Cuantía	Seguros	1.00	Unidad	11,000.00	11,000.00		C2 C3

7132 SERVICIOS DE SEGUROS DE ENFERMEDAD Y DE ACCIDENTES
7133 SERVICIOS DE SEGUROS DISTINTOS DE LOS SEGUROS DE VIDA (EXCEPTO SERVICIOS DE REASEGUROS)
71331 SERVICIOS DE SEGUROS DE VEHICULOS DE MOTOR
- 71331.00 SERVICIOS DE CONCERTACION DE POLIZAS DE SEGURO QUE CUBRAN LOS RIESGOS RELACIONADOS CON LA UTILIZACION DE VEHICULOS DE MOTOR, INCLUIDOS LOS UTILIZADOS PARA EL TRANSPORTE REMUNERADO DE PASAJEROS. LOS R

71332 SERVICIOS DE SEGUROS DE TRANSPORTE MARITIMO, TRANSPORTE AEREO Y OTROS TIPOS DE TRANSPORTE
- 71332.00 SERVICIOS DE CONCERTACION DE POLIZAS DE SEGURO QUE CUBRAN LOS RIESGOS RELACIONADOS CON LA UTILIZACION DE: EMBARCACIONES DE PASAJEROS Y DE CARGA, TANTO SI FUNCIONAN EN AGUAS MARITIMAS COMO SI FUNCIONA

71333 SERVICIOS DE SEGUROS DE FLETE
- 71333.00 SERVICIOS DE CONCERTACION DE POLIZAS DE SEGURO QUE ABARQUEN LOS RIESGOS DE PERDIDA O DANO DE LA CARGA, ADEMAS DE LA COBERTURA PROPORCIONADA POR LA EMPRESA DE TRANSPORTE

71334 OTROS SERVICIOS DE SEGUROS CONTRA DANOS A LOS BIENES

Fuente: Servicio Nacional de Contratación Pública (2016)**.** *PAC 2016 GAD Municipal del Cantón San Pedro de Pelileo.* Recuperado de: https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/buscarPACe.cpe?entidadPac=Si1mDZvTcoFxX318fjj9VqLsSMFeFHq1e3_5vCctr-g,&anio=ZPCKDty9dARNyYfX2G4yVLYnhYZETq-x1cgvyrudCuw,&nombre=CQ7ztMPFTbYqeEOnB-MqifNIYffsXCE39dzXatk0QN92yM1JT4ShFVdwOqjUXr79fkS9A-8mwPyuTiK0BU9ILwtsF0eOagv2_t4n4mPjR7DAqjXKk5Rh3MAqKjcOJTHI